

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2002 年 11 月 21 日 (21.11.2002)

PCT

(10) 国際公開番号  
WO 02/093361 A1

- (51) 国際特許分類: G06F 9/06,  
13/00, 9/445, 17/60, H04L 9/10
- (21) 国際出願番号: PCT/JP02/04643
- (22) 国際出願日: 2002 年 5 月 14 日 (14.05.2002)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:  
特願2001-143810 2001 年 5 月 14 日 (14.05.2001) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 夏野 剛 (NAT-SUNO, Takeshi) [JP/JP]; 〒100-6150 東京都千代田区永

田町二丁目11番1号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 山本 正明 (YAMAMOTO, Masaaki) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 鷺尾 諭 (WASHIO, Satoshi) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 川端 博史 (KAWABATA, Hiroshi) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP).

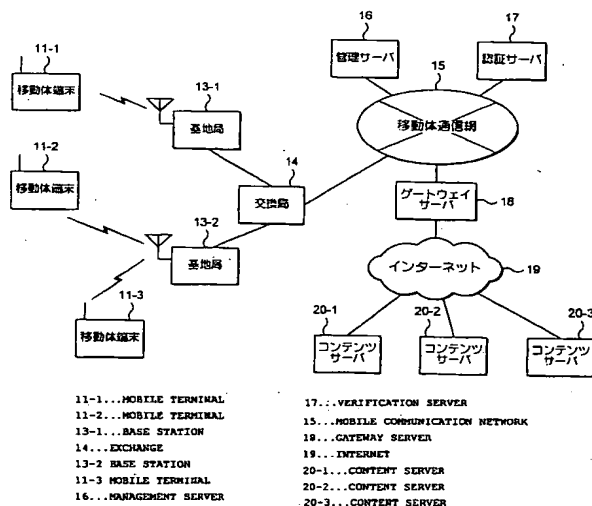
(74) 代理人: 川崎 研二 (KAWASAKI, Kenji); 〒103-0027 東京都中央区日本橋一丁目2番10号 東洋ビルディング 7階 朝日特許事務所 Tokyo (JP).

(81) 指定国 (国内): AU, BR, CA, CN, ID, IN, JP, KR, NO, NZ, PH, PL, SG, US.

[続葉有]

(54) Title: SYSTEM FOR MANAGING PROGRAM STORED IN STORAGE BLOCK OF MOBILE TERMINAL

(54) 発明の名称: 移動体端末の記憶部に格納されたプログラムを管理するシステム



(57) Abstract: In response to a request from a mobile terminal (11), a management server (16) fetches an application program from a content server (20) and delivers the fetched application program to the mobile terminal (11) together with information related to reliability of the application program. The mobile terminal (11) receives the application program from the management server (16) and by using the information related to the reliability of the application program, controls linkage operation with another application program. By such a linkage control between a plurality of application programs, it is possible to evade a security problem that precious information leaks due to operation of an application program of low reliability. Thus, it is possible to improve use-friendliness of a user of the mobile terminal (11) while maintaining a high information security.

[続葉有]



(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

---

(57) 要約:

管理サーバ16は、移動体端末11の要求に応じ、コンテンツサーバ20からアプリケーションプログラムを取得し、取得したアプリケーションプログラムを、そのアプリケーションプログラムの信頼性に関する情報と共に移動体端末11に配信する。移動体端末11は管理サーバ16からアプリケーションプログラムを受信すると、そのアプリケーションプログラムに対応する信頼性に関する情報を用いて、他のアプリケーションプログラムとの連係動作を制御する。そのような複数のアプリケーションプログラム間の連係制御により、価値の高い情報が信頼性の低いアプリケーションプログラムの動作により漏洩する、といった情報セキュリティ上の問題が回避され、高い情報セキュリティを維持しつつ移動体端末11のユーザの利便性を高めることが可能となる。

## 明細書

## 移動体端末の記憶部に格納されたプログラムを管理するシステム

## 5 技術分野

本発明は、移動体端末に内蔵あるいは装着された記憶部に格納されたプログラム（アプレットを含む）の管理システムに関する。

## 背景技術

- 10 近年、比較的記憶容量の大きい不揮発性メモリを内蔵し、その不揮発性メモリに出荷時には組み込まれていないアプリケーションプログラムを購入後に書き込み、そのアプリケーションプログラムを実行することのできる移動体端末が開発されている。そのような移動体端末のユーザは、不要になったアプリケーションプログラムを不揮発性メモリから消去し、新たに別のアプリケーションプログラムを不揮発性メモリに書き込むことにより、移動体端末を買い換えることなく、
- 15 新しいアプリケーションプログラムを利用することができる。

- このようなアプリケーションプログラムの書き込み可能な移動体端末として、例えばJavaバーチャルマシンを搭載したものがある。Javaバーチャルマシンを搭載した移動体端末は、Javaアプリケーション（Javaアプレットを含む）を移動通信網経由でダウンロードし、不揮発性メモリに書き込んだ後、
- 20 ダウンロードしたJavaアプリケーションを実行することができる。（以下、アプレットを含むアプリケーションプログラムを「アプリケーション」と呼ぶ。）

しかしながら、そのような移動体端末において一連の作業を行うために複数のアプリケーションを利用する必要がある場合に不便な点があった。

- 25 例えば、移動体端末のユーザが、通信販売による商品の購入を申し込むためのアプリケーションAと、商品の代金の支払いを行うためのアプリケーションBを利用する場合を考える。この場合、まず、ユーザはアプリケーションAを用いてある商品の購入を申し込む。しかし、ユーザはまだ購入した商品の代金を支払っていないため、代金の支払いに必要な情報、すなわち商品の代金、代金の振込先

銀行名および口座番号等をメモ用紙等に取り、いったんアプリケーションAを終了する。続いて、ユーザは代金の送金を行うために、アプリケーションBを起動する。このアプリケーションBを用いれば、ユーザは自分の銀行口座から指定口座への送金が可能である。従って、ユーザはアプリケーションBの画面において、先に書き取った情報を参照しながら、送金金額、振込先銀行名、口座番号等5 等を移動体端末に入力する。その後、ユーザはアプリケーションBを終了し、送金が正しく行われ、商品購入の手続きが完了したことを確かめるため、再度アプリケーションAを起動する。ユーザはアプリケーションAを用いて、例えば商品購入履歴等の画面を表示させ、先に購入の申し込みを行った商品について送金確認10 がなされていることを確認するとともに、商品の配送日などの情報を得る。

上記の例のように、従来の技術によれば、互いに機能が関連する複数のアプリケーションを利用する場合、ユーザはそれらのアプリケーションの切り替え操作を行ったり、必要な情報を入力したりする必要があった。その結果、ユーザにとって操作が面倒であったり、時間がかかったりするだけでなく、入力ミスによる15 トラブルも発生していた。

#### 発明の開示

上述した従来技術による移動体端末の不便な点を克服するために、本願発明者は、移動体端末の不揮発性メモリに書き込まれている複数のアプリケーションに20 連係した処理を行わせることに思い至った。しかしながら、あるアプリケーションが他のアプリケーションの機能やデータを自由に利用することを許すと、情報セキュリティ上の問題が発生する。

例えば、移動体端末に、ユーザのスケジュール管理を行うアプリケーションCと、メールを送受信するためのアプリケーションDが書き込まれているとする。25 アプリケーションCは、ユーザが友人に知られたくない予定に関する情報も管理している。ここで、もしアプリケーションCがアプリケーションDの機能やデータを自由に利用することを許可してしまうと、ユーザがアプリケーションDを用いて友人にメールを送る際、アプリケーションCの管理する、予定に関する情報を友人に送信してしまう危険性がある。そのようなトラブルは、ユーザの些細な

操作ミスやアプリケーションDの持つバグ等により起こりうる。従って、ユーザは安心してこれらのアプリケーションを利用することができない。

上記の例に示したような情報の漏洩や、情報の破壊、情報の不正な書き換え等は、特に個人情報や金銭情報等の価値の高い情報を扱う可能性のある移動体端末  
5 においては深刻な問題である。

この問題を克服するための方法として、本願発明者は、各アプリケーションに対し、アプリケーションの信頼性に関する情報を作成しておき、この信頼性に関する情報を用いたアプリケーション間の動作管理を行うことに考え至った。すなわち、動作確認が十分なされ、重要な情報を扱っても問題がないと判断される信頼性の高いアプリケーションに関しては、信頼性の低いアプリケーションの機能  
10 やデータの利用を許可する。一方、信頼性が低いと判断されるアプリケーションに関しては、信頼性の高いアプリケーションの機能やデータを利用することを許可しない。その結果、信頼性の低いアプリケーションが誤って信頼性の高いアプリケーションの扱うデータを漏洩したり、破壊したりすることが防止できる。

より具体的には、本発明は、移動体端末が、移動体端末において動作するプログラムを取得し、メモリに格納するプログラム取得過程と、前記移動体端末が、前記プログラムによる他のプログラムの起動および他のプログラムとの間のデータの授受の少なくとも一方の制御に用いられる連係制御情報を取得し、メモリに格納する連係制御情報取得過程と、前記移動体端末が、前記メモリに格納された  
20 1のプログラムの実行中に、他のプログラムの実行要求が発生したとき、実行中のプログラムに対応する前記連係制御情報に基づいて、他のプログラムの起動および他のプログラムとの間のデータの授受の態様を決定するプログラム制御過程とを備えることを特徴とするプログラム管理方法を提供する。

また、本発明は、配信サーバ、管理サーバ、および移動体端末を含む通信網において、配信サーバは、プログラムを格納するプログラム格納部と、前記プログラムを、前記移動体端末に配信するプログラム配信部とを備え、前記管理サーバは、前記プログラムに対応する連係制御情報を格納する連係制御情報格納部と、前記連係制御情報を、前記移動体端末に送信する連係制御情報送信部とを備え、前記移動体端末は、前記プログラムを、前記配信サーバより受信するプログラム  
25

受信部と、前記連係制御情報を、前記管理サーバより受信する連係制御情報受信部と、前記プログラムを記憶するプログラム記憶部と、前記連係制御情報を記憶する連係制御情報記憶部と、前記プログラムの1つの実行中に、他のプログラムの実行要求が発生したとき、実行中のプログラムに対応する前記連係制御情報に基づいて、他のプログラムの起動および他のプログラムとの間のデータの授受の態様を決定するプログラム制御部とを備えることを特徴とするプログラム管理システムを提供する。

また、本発明は、移動体端末を含む通信網において、前記移動体端末において、あるプログラムの実行中に、他のプログラムの実行要求が発生したとき、他のプログラムの起動および他のプログラムとの間のデータの授受の態様を決定するために用いられる連係制御情報を格納する連係制御情報格納部と、前記連係制御情報を、前記移動体端末に送信する連係制御情報送信部とを備えることを特徴とする管理サーバを提供する。

また、本発明は、プログラムを記憶するプログラム記憶部と、連係制御情報を記憶する連係制御情報記憶部と前記プログラムの実行中に、他のプログラムの実行要求が発生したとき、前記連係制御情報に基づいて、他のプログラムの起動および他のプログラムとの間のデータの授受の態様を決定するプログラム制御部とを備えることを特徴とする移動体端末を提供する。

また、本発明は、通信網に含まれる移動体端末において、あるプログラムの実行中に、他のプログラムの実行要求が発生したとき、他のプログラムの起動および他のプログラムとの間のデータの授受の態様を決定するために用いられる連係制御情報を、前記移動体端末に送信する連係制御情報送信処理を管理サーバのコンピュータに実行させるプログラム、およびそのプログラムを記録した記録媒体を提供する。

また、本発明は、連係制御情報を取得する連係制御情報取得処理と、あるプログラムの実行中に、他のプログラムの実行要求が発生したとき、前記連係制御情報に基づいて、他のプログラムの起動および他のプログラムとの間のデータの授受の態様を決定するプログラム制御処理とを移動体端末のコンピュータに実行させるプログラム、およびそのプログラムを記録した記録媒体を提供する。

これらのプログラム管理方法、プログラム管理システム、管理サーバ、移動体端末、プログラム、もしくは記録媒体を用いることにより、移動体端末における複数のプログラム間における関係処理が、関係制御情報に従い各プログラムの信頼性に応じて制御されるので、複数のプログラムの関係処理を行った際、情報の漏洩等によるセキュリティ低下が防がれる。

#### 図面の簡単な説明

図 1 は、本発明の第 1 実施形態および第 2 実施形態に係るアプリケーション配信システムの全体構成を示すブロック図である。

10 図 2 は、本発明の第 1 実施形態および第 2 実施形態に係る移動体端末の外観図である。

図 3 は、本発明の第 1 実施形態および第 2 実施形態に係る移動体端末の概要構成ブロック図である。

15 図 4 は、本発明の第 1 実施形態および第 2 実施形態に係る移動体端末のメモリの構成図である。

図 5 は、本発明の第 1 実施形態および第 2 実施形態に係る管理サーバの概要構成を示すブロック図である。

図 6 は、本発明の第 1 実施形態および第 2 実施形態に係るアプリケーションの情報管理システムの構成を示す図である。

20 図 7 は、本発明の第 1 実施形態および第 2 実施形態に係る、ユーザ情報格納部に格納されるデータ例を示す図である。

図 8 は、本発明の第 1 実施形態に係る、アプリケーション情報格納部の登録アプリケーション領域に格納されるデータ例を示す図である。

25 図 9 は、本発明の第 1 実施形態および第 2 実施形態に係る、アプリケーション情報格納部の一時保管アプリケーション領域に格納されるデータ例を示す図である。

図 10 および図 11 は、本発明の第 1 実施形態および第 2 実施形態に係る管理サーバにおけるアプリケーションの格納処理のフローを示す図である。

図 12 および図 13 は、本発明の第 1 実施形態および第 2 実施形態に係る、管

理サーバに公開されているアプリケーションの購入の際に移動体端末に表示される画面を示す図である。

図 1 4 および図 1 5 は、本発明の第 1 実施形態および第 2 実施形態に係る、管理サーバに公開されているアプリケーションの購入処理のフローを示す図である。

5 図 1 6 および図 1 7 は、本発明の第 1 実施形態および第 2 実施形態に係る、信頼度を付されているが管理サーバに公開されていないアプリケーションの購入処理のフローを示す図である。

図 1 8、図 1 9、および図 2 0 は、本発明の第 1 実施形態および第 2 実施形態に係る、信頼度を与えられていないアプリケーションの購入処理のフローを示す  
10 図である。

図 2 1 および図 2 2 は、本発明の第 1 実施形態および第 2 実施形態に係る、アプリケーションのダウンロードの際に移動体端末に表示される画面を示す図である。

図 2 3、図 2 4、および図 2 5 は、本発明の第 1 実施形態および第 2 実施形態  
15 に係る、アプリケーションのダウンロード処理のフローを示す図である。

図 2 6 は、本発明の第 1 実施形態および第 2 実施形態に係る、アプリケーションの起動操作の際に移動体端末に表示される画面を示す図である。

図 2 7、図 2 8、図 2 9、図 3 0、および図 3 1 は、本発明の第 1 実施形態に係る、複数のアプリケーションが連係できない場合に移動体端末に表示される画面  
20 面を示す図である。

図 3 2、図 3 3、および図 3 4 は、本発明の第 1 実施形態に係る、複数のアプリケーションが連係して動作する場合に移動体端末に表示される画面を示す図である。

図 3 5 は、本発明の第 2 実施形態に係る、アプリケーション間の権限情報を例  
25 示した図である。

図 3 6 は、本発明の第 2 実施形態に係る、アプリケーション情報格納部の登録アプリケーション領域に格納されるデータ例を示す図である。

図 3 7 は、本発明の第 3 実施形態に係る、アプリケーション情報格納部の登録アプリケーション領域に格納されるデータ例を示す図である。



図 38 は、本発明の第 3 実施形態に係るアプリケーションの情報管理システムの構成を示す図である。

図 39 は、本発明の第 3 実施形態に係る、ユーザ情報格納部に格納されるデータ例を示す図である。

- 5      図 40、図 41、および図 42 は、本発明の第 3 実施形態に係る、アプリケーションの購入処理およびダウンロード処理のフローを示す図である。

発明を実施するための最良の形態

次に本発明の望ましい実施形態について説明する。

10      [1] 第 1 実施形態

         [1. 1] 構成

         [1. 1. 1] アプリケーション配信システムの全体構成

図 1 は本発明の実施形態に係るアプリケーション配信システムの全体構成の概要を示すブロック図である。

- 15      アプリケーション配信システムは、複数の移動体端末 11-1、11-2、・・・と、複数の基地局 13-1、13-2、・・・と、複数の交換局 14 と、移動体通信網 15 と、管理サーバ 16 と、認証サーバ 17 と、ゲートウェイサーバ 18 と、インターネット 19 と、複数のコンテンツサーバ 20-1、20-2、・・・とにより構成されている。なお、以下では、特に区別する必要がない場合に、各移動
- 20      体端末を移動体端末 11 と、各基地局を基地局 13 と、また各コンテンツサーバをコンテンツサーバ 20 と総称する。

- 移動体端末 11 は、例えば携帯電話、PHS (Personal Handy  
phone System; 登録商標) 等の無線通信機能を有する情報処理装置  
である。移動体端末 11 は、アプリケーションを記憶可能な不揮発性メモリを内  
蔵しているか、もしくはアプリケーションを記憶可能な外部の不揮発性メモリを  
25      装着することができる。移動体端末 11 は、管理サーバ 16 より移動体通信網 15、交換局 14、および基地局 13 を介してアプリケーションをダウンロードし、ダウンロードしたアプリケーションを不揮発性メモリに書き込む。移動体端末 11 のユーザは、望む時に不揮発性メモリに書き込まれたアプリケーションを実行

することができる。

基地局 1 3 は有線により交換局 1 4 を介して移動体通信網 1 5 に接続されている。基地局 1 3 は、割り当てられた無線ゾーン内に存在する移動体端末 1 1 のいずれかが移動体通信網 1 5 に対して発呼する場合、もしくは割り当てられた無線  
5 ゾーン内に存在する移動体端末 1 1 のいずれかに対して移動体通信網 1 5 から発呼がされた場合、該当する移動体端末 1 1 との間で無線接続を確立し、移動体端末 1 1 と移動体通信網 1 5 との間の通信を中継する。なお、基地局 1 3 は割り当てられた無線ゾーン内の移動体端末 1 1 との間で頻繁に無線による制御信号をやりとりを行うことにより、割り当てられた無線ゾーン内にどの移動体端末 1 1 が  
10 存在するかを把握し、その情報を移動体端末 1 1 の位置情報として移動体通信網 1 5 に送信する。

交換局 1 4 は、基地局 1 3 および移動体通信網 1 5 とそれぞれ有線により接続されており、基地局 1 3 と無線接続を確立した移動体端末 1 1 と、移動体通信網 1 5 との間に利用可能な通信経路を確立する装置である。なお、移動体通信網 1  
15 5 との間に通信状態を確立した移動体端末 1 1 が、ある交換局 1 4 の管理する無線ゾーンから他の交換局 1 4 の管理する無線ゾーンに移動した場合には、交換局 1 4 は、確立されている通信状態を維持しつつ、交換局間の通信接続切替制御を行う。

移動体通信網 1 5 は、交換局 1 4 を閥門交換局（図示略）を介して有線により  
20 相互に接続した通信網である。移動体通信網 1 5 は、交換局 1 4 および基地局 1 3 を介して複数の移動体端末 1 1 間の通信経路を確立する。また、移動体通信網 1 5 は固定電話網等の他の通信網（図示略）と接続されている。さらに、移動体通信網 1 5 はゲートウェイサーバ 1 8 を介してインターネット 1 9 に接続されている。なお、移動体通信網 1 5 内には位置登録メモリ（図示略）が設けられてお  
25 り、この位置登録メモリには各基地局 1 3 から得られる移動体端末 1 1 の位置情報が記録される。移動体通信網 1 5 は、特定の移動体端末 1 1 に対する発呼を行う場合には、位置登録メモリに記録された情報を用いて、該当する移動体端末 1 1 と無線接続の可能な基地局 1 3 に対し接続要求を行う。

管理サーバ 1 6 は、移動体端末 1 1 の要求に応じて、アプリケーションを移動

体端末 11 に配信するサーバである。管理サーバ 16 は、アプリケーションの移動体端末 11 への配信に先立ち、アプリケーションの配信元であるコンテンツサーバ 20 からアプリケーションの送信を受け、送信されたアプリケーションをデータベースに格納する。

- 5      管理サーバ 16 の管理事業者は、コンテンツサーバ 20 の管理事業者の希望があれば、コンテンツサーバ 20 が管理しているアプリケーションの内容を審査し、そのアプリケーションに対し、移動体端末 11 における動作の安全性等の観点から信頼度を決定する。決定された信頼度は、管理サーバ 16 のデータベースに記録される。管理サーバ 16 は、信頼度の与えられたアプリケーションの配信要求
- 10      を移動体端末 11 から受けると、移動体端末 11 に対し、アプリケーションと共にその信頼度を送信する。

- 移動体端末 11 がアプリケーションを利用するには、アプリケーションの購入、アプリケーションの移動体端末 11 に対するダウンロード、およびダウンロードされたアプリケーションを利用可能な状態にする処理(以下、「アクティベーション処理」と呼ぶ)が必要である。管理サーバ 16 は、移動体端末 11 のユーザによってアプリケーションの購入が要求されると、要求されたアプリケーションの配信準備を行う。また、管理サーバ 16 は、移動体端末 11 にアプリケーションがダウンロードされる際、移動体端末 11 のメモリにおけるアプリケーションの書き込み領域を決定し、移動体端末 11 に対しアプリケーションの書き込みを許可する。さらに、管理サーバ 16 は、移動体端末 11 に対し、移動体端末 11 におけるアプリケーションのアクティベーション処理の指示を行う。管理サーバ 16 はアプリケーションの配信準備およびアクティベーション処理を行うと、それらの処理に関する情報を、移動体通信網 15 に接続された課金管理サーバ(図示略)に送信する。課金管理サーバは管理サーバ 16 より配信準備およびアクティベーション処理に関する情報を受信すると、それらの情報を用いて、処理の対象の移動体端末 11 に対する、アプリケーションの利用料金算出を行う。
- 15
- 20
- 25

認証サーバ 17 は、各移動体端末 11、管理サーバ 16、各コンテンツサーバ 20、および認証サーバ 17 自身の公開鍵方式における公開鍵を管理するサーバである。認証サーバ 17 は、任意の移動体端末 11、管理サーバ 16、および任

意のコンテンツサーバ 20 からの要求に応じて、送信要求のされた公開鍵を送信要求を行った装置に送信する。

コンテンツサーバ 20 は、移動体端末 11 の仕様に応じて開発されたアプリケーションを 1 または複数管理しており、管理サーバ 16 からの要求に応じて、該当するアプリケーションを管理サーバ 16 に送信する。なお、コンテンツサーバ 20 の管理事業者は、希望すればアプリケーションを管理サーバ 16 の管理事業者に送信し、その内容の審査を依頼し、審査結果に応じて管理サーバ 16 の管理事業者からアプリケーションに対応する信頼度を取得することができる。

#### [1. 1. 2] 移動体端末の構成

次に移動体端末 11 の構成について説明する。なお、ここでは移動体端末 11-1 を例に説明する。

図 2 は移動体端末 11-1 の外観図である。また、図 3 は移動体端末 11-1 の概要構成を示したブロック図である。図 3 に示すように、移動体端末 11-1 は、ディスプレイ部 21、操作部 22、アンテナ 34A、制御部 31、制御用メモリ 32、通信部 34、メモリコントローラ 35、メモリ 12 および音声入出力部 36 を備えている。

ディスプレイ部 21 は、移動体端末 11-1 のユーザに移動体端末 11-1 の制御部がメッセージを表示するための構成部である。ディスプレイ部 21 には、図 2 に示されているアプリケーション実行のための処理メニューの他、種々の処理メニュー、情報サイトから得られる情報を表示するブラウザ画面、電波強度や電話番号等の各種情報が表示される。

操作部 22 は、制御部 31 に対し、指示を与える構成部である。操作部 22 には、数字等の示された操作ボタンおよびアプリボタン 23 が設けられている。アプリボタン 23 はアプリケーションの操作を簡便に行うための機能が割り当てられた操作ボタンである。

アンテナ 34A は、移動体端末 11-1 が無線通信を行う際、電波を物理的に出力および入力する構成部である。

制御部 31 は、移動体端末 11-1 において、メモリ 12 を除く各構成部の制御を行うマイクロプロセッサである。制御部 31 は、制御用メモリ 32 に記憶さ

れている制御用プログラムに従って各構成部の制御を行う。また、制御部 31 は、メモリコントローラ 35 を介してメモリ 12 からアプリケーションを読み出し、読み出したアプリケーションを実行する。制御部 31 は、実行中の制御用プログラムおよびアプリケーションからの要求により、メモリ 12 に書き込まれているアプリケーションもしくはデータを利用することがある。その場合、制御部 31 はメモリコントローラ 35 にアプリケーションもしくはデータの利用要求とこの利用要求の発信元である制御用プログラムもしくはアプリケーションの識別情報を送信する。この識別情報は、メモリコントローラ 35 が利用要求に応じるか否かを判定する際に利用される。制御部 31 は制御用プログラムもしくはアプリケーションを複数同時に実行することがあるが、制御用プログラムとアプリケーションの間、もしくは複数のアプリケーションの間でデータの受け渡しを直接行うことはなく、必ずメモリコントローラ 35 を介してデータの受け渡しを行う。

制御用メモリ 32 は制御部 31 の制御用プログラムおよび制御用プログラムが管理するデータを記録するための揮発性メモリおよび不揮発性メモリである。また、制御用メモリ 32 は、制御部 31 が制御用プログラムを実行する際の作業領域としても利用される。なお、制御用プログラムには、移動体端末 11-1 が出荷時に有している電話番号記録機能等の基本機能を実現するプログラムも含まれている。

通信部 34 は、アンテナ 34A を介して基地局 13 との間で電波による信号の送受信を行う構成部である。通信部 34 は、移動体端末 11-1 が基地局 13 に送信したい情報を持つ場合、制御部 31 の制御のもとで、ベースバンド信号を送信したいデジタルデータを示す信号により変調した後、アンテナ 34A に印加することにより、電波信号を基地局 13 に送信する。また、通信部 34 はアンテナ 34A を介して基地局 13 より電波を受信すると、受信した電波からアプリケーションまたはデータを復調し、アプリケーションについてはメモリコントローラ 35 に、復調されたデータのうちデジタル音声データについては音声入出力部 36 に、制御データ等のその他のデータは制御部 31 に、それぞれ送信する。

音声入出力部 36 は移動体端末 11-1 のユーザが他の移動体端末 11 や固定電話等のユーザとの間で会話をする際、音声の入出力処理を行う。音声入出力部

36はマイク（図示略）、A/Dコンバータ（図示略）、D/Aコンバータ（図示略）、スピーカ（図示略）等を有している。移動体端末11-1のユーザが話す場合、音声入出力部36はマイクから移動体端末11-1のユーザの声をアナログ信号として取り込み、取り込んだアナログ信号をA/Dコンバータによりデジタル信号に変換後、通信部34に送信する。一方、移動体端末11-1のユーザの会話の相手が話す場合、通信部34から送信されるデジタル音声データをD/Aコンバータによりアナログ信号に変換し、スピーカから発音する。

メモリコントローラ35はメモリ12と制御部31および通信部34との間のデータの送受信を制御するためのマイクロプロセッサである。メモリコントローラ35は、通信部34からアプリケーションが送信されると、アプリケーションをメモリ12に書き込む。通信部34から送信されるアプリケーションには、管理サーバ16からの書き込み要求と共に、メモリ12においてアプリケーションを書き込むべきメモリエリアが指定されており、メモリコントローラ35は指定されたメモリエリアにアプリケーションを書き込む。また、メモリコントローラ35が通信部34から受信するアプリケーションが、ある程度以上の信頼度が与えられているアプリケーションである場合、メモリコントローラ35はアプリケーションと共にその信頼度も受信する。その場合、メモリコントローラ35はアプリケーションを書き込むメモリエリアに、受信した信頼度も書き込む。

メモリコントローラ35は、制御部31からメモリ12に書き込まれているアプリケーションもしくはデータの利用要求、すなわち読み取り要求、書き込み要求、もしくは削除要求を受信すると、その利用要求を承諾すべきかどうかを判定し、その判定の結果に基づいてメモリ12に対する処理を行う。制御部31のメモリ12に書き込まれているアプリケーションもしくはデータの利用要求は、利用要求を行っているプログラムの識別情報を伴っている。メモリコントローラ35は利用要求を受信すると、まずその利用要求を行っているプログラムの信頼度を確認する。利用要求を行っているプログラムが制御部31の管理する制御用プログラムである場合、制御用プログラムには最も高い信頼度が与えられているため、メモリコントローラ35は無条件に利用要求を承諾し、利用要求に従ったメモリ12に対する処理を行う。利用要求を行っているプログラムがメモリ12

から読み出されたアプリケーションである場合、メモリコントローラ 35 は識別情報から、利用要求を行っているアプリケーションの書き込まれているメモリエリアを特定し、そのアプリケーションに与えられている信頼度を読み出す。なお、アプリケーションの信頼度が不明である場合、メモリコントローラ 35 は、そのアプリケーションを信頼度が最も低いものとして扱う。続いて、メモリコントローラ 35 は、利用要求の対象となっているアプリケーションもしくはデータの書き込まれているメモリエリアから同様に信頼度を読み出す。メモリコントローラ 35 はこうして得られる 2 つの信頼度を比較し、利用要求を行っているアプリケーションの信頼度が、利用要求の対象となっているアプリケーション、もしくは利用要求の対象となっているデータを管理しているアプリケーションの信頼度より高いか、もしくは同等の場合に限り、利用要求を承諾し、利用要求に従ったメモリ 12 に対する処理を行う。この信頼度を用いた制御処理については、具体例を挙げて後述する。

また、メモリコントローラ 35 は、移動体端末 11-1 の秘密鍵および公開鍵の生成、および秘密鍵を用いたデータの暗号化および復号化を行う。メモリコントローラ 35 は、制御部 31 の制御のもとで、移動体端末 11 のユーザの入力するキーワードに基づいて秘密鍵および公開鍵の対を作成する。メモリコントローラ 35 は生成した公開鍵を通信部 34 を介して認証サーバ 17 に送信し、一方、秘密鍵については容易に移動体端末 11-1 に漏洩しないようプロテクト処理を施した後、記録する。メモリコントローラ 35 は、通信部 34 を介して外部より移動体端末 11-1 の公開鍵で暗号化されたデータを受信すると、移動体端末 11-1 の秘密鍵を用いて暗号化されたデータを復号する。また、メモリコントローラ 35 は、メモリ 12 のデータを通信部 34 を介して外部に送信する際、必要に応じて送信するデータを移動体端末 11-1 の秘密鍵で暗号化する。

メモリ 12 は、通信部 34 を介して外部より受信されるアプリケーションおよびそれらのアプリケーションが管理するデータを記憶するための不揮発性メモリである。図 4 はメモリ 12 の構成を示した図である。

メモリ 12 は複数のメモリエリアに区画されている。これらのメモリエリアには管理エリア 40 とフリーエリア 41 がある。管理エリア 40 は管理サーバ 16

によりある程度以上の信頼度を与えられているアプリケーション用の領域であり、フリーエリア 41 は管理サーバ 16 によりある程度以上の信頼度を与えられていないアプリケーション用の領域である。管理エリア 40 は複数の管理エリア 40-1 ~ 管理エリア 40-n (n は任意の正の整数) からなり、またフリーエリア 41 は複数のフリーエリア 41-1 ~ フリーエリア 41-m (m は任意の正の整数) からなる。以下、管理エリア 40-1 およびフリーエリア 41-1 を例として説明する。

管理エリア 40-1 は、アプリケーション領域 40A-1、データ領域 40D-1、および信頼情報領域 40R-1 に区画されている。アプリケーション領域 40A-1 にはアプリケーション本体が格納される。データ領域 40D-1 には、アプリケーション領域 40A-1 に格納されるアプリケーションが管理するデータが格納される。信頼情報領域 40R-1 には、アプリケーション領域 40A-1 に格納されるアプリケーションに与えられている信頼度が格納される。

フリーエリア 41-1 は、アプリケーション領域 41A-1 およびデータ領域 41D-1 に分かれている。アプリケーション領域 41A-1 にはアプリケーション本体が格納される。データ領域 41D-1 には、アプリケーション領域 41A-1 に格納されるアプリケーションが管理するデータが格納される。

アプリケーション領域 40A-1 およびアプリケーション領域 41A-1 におけるアプリケーションの書き込みおよび削除、および信頼情報領域 40R-1 における信頼度の書き込みおよび削除は、メモリコントローラ 35 が管理サーバ 16 からの指示のみに従って行う。一方、アプリケーション領域 40A-1 およびアプリケーション領域 41A-1 におけるアプリケーションの読み出し、信頼情報領域 40R-1 における信頼度の読み出し、データ領域 40D-1 およびデータ領域 41D-1 のデータの書き込み、読み出し、および削除は、メモリコントローラ 35 の管理のもとで、制御部 31 の要求により行われる。

### [1. 1. 3] 管理サーバの構成

図 5 は管理サーバ 16 の概要構成を示したブロック図である。管理サーバ 16 は、暗号鍵格納部 51、アプリケーション情報格納部 52、ユーザ情報格納部 53、および制御部 54 を備えている。



暗号鍵格納部 5 1 は、制御部 5 4 により生成される管理サーバ 1 6 の秘密鍵、認証サーバ 1 7 から取得される各移動体端末 1 1 および各コンテンツサーバ 2 0 の公開鍵を格納するデータベースである。

- アプリケーション情報格納部 5 2 は、各コンテンツサーバ 2 0 から送信される  
5 アプリケーション本体もしくはアプリケーションの保管場所情報をアプリケーションの名称等の情報と共に格納しているデータベースである。

- ユーザ情報格納部 5 3 は、各移動体端末 1 1 のメモリ 1 2 に書き込まれているアプリケーションに関する情報、および移動体端末 1 1 のユーザにより購入され、  
10 移動体端末 1 1 のユーザが望む時に移動体端末 1 1 にダウンロードし、メモリ 1 2 に書き込み可能なアプリケーションに関する情報を格納しているデータベースである。

- 制御部 5 4 は、管理サーバ 1 6 の各構成部の制御を行うマイクロプロセッサである。制御部 5 4 は認証サーバ 1 7 からの公開鍵の取得、コンテンツサーバ 2 0 からのアプリケーションの取得と暗号化されているアプリケーションの復号化、  
15 および移動体端末 1 1 へ配信するアプリケーションの暗号化および配信の制御を行う。また、それらの処理に伴う暗号鍵格納部 5 1、アプリケーション情報格納部 5 2、およびユーザ情報格納部 5 3 の各データベースのデータ更新を行う。

管理サーバ 1 6 の各データベースの構成およびアプリケーションの配信動作の詳細については後述する。

#### 20 [1. 1. 4] アプリケーションの情報管理システムの構成

図 6 は移動体端末 1 1、管理サーバ 1 6、およびコンテンツサーバ 2 0 におけるアプリケーションに関する情報管理のシステムを示す図である。

- ユーザ情報格納部 5 3 は、移動体端末 1 1-1、移動体端末 1 1-2、・・・、移動体端末 1 1-k (k は移動体端末 1 1 の数を表す整数) に対応するデータ格  
25 納領域として、ユーザ情報格納部 5 3-1、ユーザ情報格納部 5 3-2、・・・、ユーザ情報格納部 5 3-k を持っている。各ユーザ情報格納部 5 3-i (i=1~k) は、既配信アプリケーション領域 5 3A-i と配信可能アプリケーション領域 5 3B-i に区画されている。あるユーザ情報格納部 5 3-i の既配信アプリケーション領域 5 3A-i は、移動体端末 1 1-i のメモリ 1 2 の管理エリア

40またはフリーエリア41に現在書き込まれているアプリケーションの情報を格納する領域である。一方、ユーザ情報格納部53-iの配信可能アプリケーション領域53B-iは、現在は移動体端末11-iのメモリ12に書き込まれていないが、移動体端末11-iのユーザにより購入済みであり、移動体端末11-iの要求により、いつでも移動体端末11への配信が可能なアプリケーションの情報を格納する領域である。既配信アプリケーション領域53Aおよび配信可能アプリケーション領域53Bには、アプリケーションの名称、バージョン番号、各アプリケーションを識別する識別番号、アプリケーションのサイズ、アクティベーション処理の完了/未完了の別、アプリケーションの保管番号等の情報が格納されている。図7は移動体端末11-1に対応したユーザ情報格納部53-iに格納されているデータを例示したもので、簡略化のため、対応するメモリエリア、アプリケーションの識別番号、アクティベーション、および保管番号に関する項目のみを示している。

図7に示す例では、移動体端末11-1の管理エリア40-1におけるアプリケーション領域40A-1には、現在、識別番号が「AP-3568」であるアプリケーションが書き込まれており、アクティベーション処理がされている。保管番号は、配信準備のなされているアプリケーションの、アプリケーション情報格納部52における一時的保管場所を特定するための情報である。従って、既に移動体端末11-1に配信されているアプリケーションに関しては、保管番号は不要であるため、既配信アプリケーション領域53Aにおけるアプリケーションに関しては、保管番号は与えられない。

また、図7に示す例において、移動体端末11-1のフリーエリア41-1におけるアプリケーション領域41A-1には、現在、識別番号が「F-0325」であるアプリケーションが書き込まれており、アクティベーション処理がされている。

さらに、図7に示す例において、移動体端末11-1のユーザは、現在、メモリ12に書き込んではいないが、既に購入しており、いつでもダウンロード可能なアプリケーションとして、4つのアプリケーションを持っている。例えば、それらのアプリケーションの1つである識別番号が「AP-4125」であるアプ

リケーションはその本体が、現在、アプリケーション情報格納部 5 2 において保管番号「T-7851」で識別される領域に格納されている。それに対し、識別番号が「AP-3021」であるアプリケーションは、保管番号に「削除済み」との記録があることから、アプリケーション情報格納部 5 2 には現在、アプリケーション本体が格納されていない。さらに、識別番号が「AP-4513」であるアプリケーションは、保管番号にデータが与えられていないことから、このアプリケーションは管理サーバ 1 6 の登録アプリケーション領域 5 2 R に格納されているアプリケーションであり、そもそも保管番号を持つ必要がないものである。なお、配信可能アプリケーション領域 5 3 B に情報の格納されているアプリケーションは、現在移動体端末 1 1-1 のメモリ 1 2 に書き込まれていないことから、当然ながらアクティベーション処理は行われておらず、従ってアクティベーションに関する項目にはデータが与えられていない。

アプリケーション情報格納部 5 2 は、図 6 に示すように、登録アプリケーション領域 5 2 R および一時保管アプリケーション領域 5 2 T から構成されている。登録アプリケーション領域 5 2 R には、移動体端末 1 1 用に開発された様々なアプリケーションに関して、アプリケーションの名称、バージョン番号、各アプリケーションの識別番号、アプリケーションのサイズ、利用料金、アプリケーションの機能概要等の情報がアプリケーション本体もしくはアプリケーションの保管場所情報と共に格納されている。また、ある程度以上の信頼度が与えられているアプリケーションに関しては、信頼度、アプリケーションの公開／非公開の別、料金徴収の管理サーバ 1 6 の管理事業者による代行／非代行の別等の情報も格納されている。なお、ある程度以上の信頼度の与えられていないアプリケーションに関しては、登録アプリケーション領域 5 2 R の信頼度の項目には、信頼度として「0」が格納されている。図 8 は登録アプリケーション領域 5 2 R に格納されるデータを例示したもので、簡略化のため、アプリケーションの識別番号、信頼度、公開、料金徴収、および保管場所に関する項目のみが示されている。アプリケーションの保管場所情報としては、目的のアプリケーションを含むファイルの所在を特定可能な情報であれば何でもよいが、例えばインターネットにおいて広く利用されている URL (Uniform Resource Locator)

が利用可能である。

図 8 に例示した登録アプリケーション領域 5 2 R の情報によれば、例えば識別番号が「A P - 3 5 6 8」のアプリケーションの信頼度は「3」、アプリケーションは管理サーバ 1 6 において公開し、料金徴収は管理サーバ 1 6 の管理事業者が代行し、そのアプリケーション本体は登録アプリケーション領域 5 2 R 内に格納されていることが分かる。一方、識別番号が「A P - 3 7 1 2」のアプリケーションの信頼度は「5」、アプリケーションは公開し、料金徴収は管理サーバ 1 6 の管理事業者が代行せず、そのアプリケーションはアプリケーション情報格納部 5 2 内には格納されておらず、`ftp://ftp.abc_software.com/application`という場所に、`ap_0306.exe`というファイル名で保管されていることが分かる。また、識別番号が「F - 3 2 5 1」であるアプリケーションは、信頼度が与えられていないアプリケーションであり、従って公開および料金徴収に関する項目にはデータが与えられていない。なお、アプリケーションの公開／非公開、料金徴収の代行／非代行、およびアプリケーションの保管場所の違いについては後述する。

一時保管アプリケーション領域 5 2 T には、登録アプリケーション領域 5 2 R においてアプリケーションの保管場所情報が登録されているアプリケーションに関し、移動体端末 1 1 より配信の要求があった際、それらのアプリケーションの配信元であるコンテンツサーバ 2 0 からアプリケーション本体を受信した後、移動体端末 1 1 に配信が行われるまでの間、それらのアプリケーション本体が一時的に格納されている。図 9 は一時保管アプリケーション領域 5 2 T に格納されるデータ構造を例示したもので、アプリケーション本体は一時保管アプリケーション領域 5 2 T においてそれらを特定するための保管番号と関連づけて格納されている。

## 25 [1. 2] 配信処理の概要

続いて、アプリケーションの配信処理の流れを説明する。

### [1. 2. 1] アプリケーション購入前の処理

#### [1. 2. 1. 1] 暗号鍵の発行

本発明の実施形態に係るアプリケーション配信システムにおいては、移動体通

信網 15 の管理事業者、管理サーバ 16 の管理事業者、およびコンテンツサーバ 20 の管理事業者のいずれからも独立した事業者により管理される認証サーバ 17 により、公開鍵方式による公開鍵の管理が行われる。

まず、認証サーバ 17 は、認証サーバ 17 自身の秘密鍵「SK-AS」(Secret Key for Authentication Server) および公開鍵「PK-AS」(Public Key for Authentication Server) の対を生成し、秘密鍵「SK-AS」については外部に漏洩することのないよう保管し、公開鍵「PK-AS」に関しては任意の外部の装置からの要求に応じて送信を行う。

- 10 各移動体端末 11 においては、ユーザの操作に応じて秘密鍵「SK-MT」(Secret Key for Mobile Terminal) および公開鍵「PK-MT」(Public Key for Mobile Terminal) の対が作成される。秘密鍵「SK-MT」については各移動体端末 11 のメモリコントローラ 35 により外部に漏洩がないよう管理されている。一方、各
- 15 移動体端末 11 は、作成した公開鍵「PK-MT」を移動体通信網 15 を介して認証サーバ 17 に送信する。認証サーバ 17 は、移動体端末 11 から公開鍵「PK-MT」を受信すると、受信した公開鍵「PK-MT」を各移動体端末 11 の識別番号と関連づけてデータベースに格納する。この公開鍵「PK-MT」は、認証サーバ 17 の公開鍵「PK-AS」と同様に、任意の装置からの要求に応じて、
- 20 認証サーバ 17 により送信される。

個々の移動体端末 11 の秘密鍵および公開鍵を区別する場合には、上記の呼称に移動体端末 11 の添字番号を付ける。例えば、移動体端末 11-1 の秘密鍵は「SK-MT-1」と呼ぶ。

- 管理サーバ 16 および各コンテンツサーバ 20 は、各移動体端末 11 と同様に、
- 25 秘密鍵および公開鍵の対を作成し、秘密鍵については外部に漏洩することのないよう保管する一方、公開鍵に関しては認証サーバ 17 に送信する。認証サーバ 17 は、管理サーバ 16 から公開鍵を受信すると、受信した公開鍵を管理サーバ 16 の識別番号と関連づけてデータベースに格納する。コンテンツサーバ 20 から公開鍵が受信された場合も同様である。管理サーバ 16 やコンテンツサーバ 20

の公開鍵は、認証サーバ17および移動体端末11の公開鍵と同様に、任意の装置からの要求に応じて、認証サーバ17により送信される。この明細書では管理サーバ16およびコンテンツサーバ20用の秘密鍵および公開鍵を以下のように呼ぶこととする。

5        管理サーバ16の秘密鍵：「SK-MS」(Secret Key for Management Server)

         管理サーバ16の公開鍵：「PK-MS」(Public Key for Management Server)

         コンテンツサーバ20の秘密鍵：「SK-CS」(Secret Key for Contents Server)

         コンテンツサーバ20の公開鍵：「PK-CS」(Public Key for Contents server)

         また、個々のコンテンツサーバ20用の秘密鍵および公開鍵を区別する場合には、移動体端末11の場合と同様に、上記の呼称にコンテンツサーバ20の添字番号を付ける。例えば、コンテンツサーバ20-1用の秘密鍵は「SK-CS-1」と呼ぶ。

         なお、認証サーバ17、各移動体端末11、管理サーバ16および各コンテンツサーバ20は、それぞれの秘密鍵を用いた暗号化アルゴリズムと、公開鍵を用いた復号化アルゴリズムとが共通しているため、それぞれの装置は鍵を交換することにより、相互にデータの暗号化および復号化が可能である。

#### [1. 2. 1. 2] アプリケーションの審査

         コンテンツサーバ20の管理事業者は、自分が管理をしているアプリケーションが他のアプリケーションとの関係を行う必要がある場合や、高い価値を有する情報を扱うものである場合には、それらのアプリケーションにある程度以上の信頼度を与えるよう、管理サーバ16の管理事業者に対しアプリケーションの内容審査を依頼することができる。

         管理サーバ16の管理事業者は、コンテンツサーバ20の管理事業者よりアプリケーションの内容審査の依頼を受けると、そのアプリケーションの利用目的、アプリケーションの動作内容、コンテンツサーバ20の管理事業者によるアプリ

ケーションの管理体制等を審査し、その結果に応じて審査したアプリケーションに対し信頼度を与える。信頼度の区分方法にはさまざまな方法が考えられるが、以下の説明においては簡単化のため、審査によって与えられる信頼度は「1」、  
「2」、「3」、「4」、「5」の5段階とし、数が大きいほど信頼度が高いものとする。  
5     る。なお、審査が行われていないアプリケーションに関しては、信頼度「0」が与えられるものとする。

例えば、信頼度「5」の与えられたアプリケーションは、管理サーバ16の管理事業者により、コンテンツサーバ20の管理事業者による管理体制やアプリケーションの動作の安定性等が検証され、必要に応じて、移動体端末11の制御用  
10     プログラム、制御用メモリ32に格納されているデータ、メモリ12に格納されているアプリケーションおよびデータを利用できる。それらのデータの中には、移動体端末11のユーザの個人情報やクレジットカード番号等の高い価値を有する情報が含まれている可能性がある。

それに対し、例えば信頼度「1」の与えられたアプリケーションは、アプリケーションの動作は安定しているが、そのアプリケーションがそもそも個人情報や  
15     金銭情報等の高い価値を持ったデータの利用を目的としていないため、低い信頼度で動作上の問題がない、と判断されたアプリケーションや、コンテンツサーバ20の管理事業者によるデータ管理体制が不十分等の理由で、高い価値を持ったデータを扱うとデータ漏洩等の危険性がある、と判断されたアプリケーションで  
20     ある。信頼度「1」の与えられたアプリケーションは、他の信頼度「1」を与えられたアプリケーション、もしくは信頼度が「0」であるアプリケーションとの間では連係動作を行うことができる。しかしながら、信頼度「1」の与えられたアプリケーションは、信頼度が「2」、「3」、「4」、もしくは「5」であるアプリケーションに対してデータを渡したり、機能を提供することはできるが、それら  
25     のアプリケーションからデータを受け取ったり、それらのアプリケーションの機能を利用することはできない。また、移動体端末11の制御用プログラムの機能を利用したり、制御用メモリ32に格納されたデータを利用することも一切できない。

管理サーバ16の管理事業者は、アプリケーションに対して「1」以上の信頼

度を与えた場合には、管理サーバ16の登録アプリケーション領域52Rに、そのアプリケーションの識別番号等と共に信頼度を登録する。

〔1. 2. 1. 3〕管理サーバに対するアプリケーションの公開依頼

コンテンツサーバ20の管理事業者は、「1」以上の信頼度の与えられたアプリケーションの移動体端末11に対する公開を管理サーバ16に依頼することができる。公開を依頼されたアプリケーションは、管理サーバ16の登録アプリケーション領域52Rにおける公開に関する項目が「Yes」と登録される。管理サーバ16は各移動体端末11から購入可能なアプリケーション情報一覧の送信要求を受信すると、登録アプリケーション領域52Rにおける公開に関する項目が「Yes」であるアプリケーションの情報を移動体端末11に送信する。その結果、移動体端末11のユーザは公開依頼のされているアプリケーションを容易に見つけることができ、また容易に購入の手続きを行うことができる。

一方、公開されていないアプリケーションに関しては、移動体端末11のユーザは例えば配信元のコンテンツサーバ20内のホームページを介して、直接コンテンツサーバ20の管理事業者に対し申込みを行うことにより、購入を行う。従って、コンテンツサーバ20の管理事業者が、自ら定めた一定の条件を満たす移動体端末11に対してのみ、アプリケーションの配信を行いたいような場合には、アプリケーションの公開を管理サーバ16に対して依頼しない方が好都合である。なお、アプリケーションが管理サーバ16において公開されない場合も、アプリケーションは管理サーバ16経由で移動体端末11に配信され、管理サーバ16によりアプリケーション情報の管理が行われる点には変わりがない。

〔1. 2. 1. 4〕管理サーバに対する料金徴収代行依頼

コンテンツサーバ20の管理事業者は、「1」以上の信頼度の与えられたアプリケーションに関して、管理サーバ16に対し、その利用料金の徴収代行を依頼することができる。利用料金の徴収代行の依頼をされたアプリケーションは、管理サーバ16の登録アプリケーション領域52Rにおける料金徴収に関する項目が「Yes」と登録される。

管理サーバ16は各移動体端末11から料金徴収に関する項目が「Yes」であるアプリケーションの購入要求を受けると、アプリケーションの情報が管理サ



- サーバ16の配信可能アプリケーション領域53Bに書き込まれた時点で、アプリケーションの識別番号、移動体端末11の識別番号、および購入日時等の情報を移動体通信網15に接続された課金管理サーバに送信する。同様に、管理サーバ16は、ある移動体端末11について、料金徴収に関する項目が「Yes」であるアプリケーションのアクティベーション処理を行うと、その時点で、アプリケーションの識別番号、その移動体端末11の識別番号、および購入日時等の情報を移動体通信網15に接続された課金管理サーバに送信する。課金管理サーバは管理サーバ16から送信されるこれらの情報に基づき、該当する移動体端末11のアプリケーションの利用料金を算出する。アプリケーションの利用料金が購入時から課金されるか、アクティベーション処理の時点から課金されるかは、コンテンツサーバ20の管理事業者と管理サーバ16もしくは移動体通信網15の管理事業者の間で決められており、課金管理サーバに課金に関する情報として記録されている。課金管理サーバにより算出されるアプリケーションの利用料金は、同じく課金管理サーバにより算出される移動体端末11の通信料金と共に、移動体通信網15の管理事業者により移動体端末11のユーザから徴収される。その後、移動体通信網15の管理事業者は各アプリケーションの提供元であるコンテンツサーバ20の管理事業者に対し、徴収したアプリケーションの利用料金から一定の徴収代行手数料を差し引いた金額を送金する。さらに、移動体通信網15の管理事業者は、得られた徴収代行手数料の一定部分を管理サーバ16の管理事業者に課金のための情報提供サービス料として送金する。

[1. 2. 1. 5] 管理サーバに対するアプリケーション格納依頼

- コンテンツサーバ20の管理事業者は、「1」以上の信頼度の与えられたアプリケーションに関して、管理サーバ16に対し、アプリケーションを管理サーバ16の登録アプリケーション領域52Rに格納するよう依頼することができる。あるアプリケーションの格納依頼が行われた場合、登録アプリケーション領域52Rの保管場所に関する項目には、そのアプリケーションの保管場所情報ではなく、アプリケーション本体が格納される。

登録アプリケーション領域52Rにおいて、アプリケーション本体を格納するか、それともアプリケーションの保管場所情報を格納するかは、管理サーバ16

とコンテンツサーバ20との間の通信速度や、アプリケーションの内容等に応じて、コンテンツサーバ20の管理事業者により決定される。アプリケーション本体を登録アプリケーション領域52Rに格納しておく、移動体端末11から管理サーバ16に対しアプリケーションの配信要求があった場合、管理サーバ16

5 はアプリケーション本体をその都度コンテンツサーバ20から送信してもらう必要がないため、迅速に移動体端末11にアプリケーションの配信を行うことができる。従って、例えば管理サーバ16とコンテンツサーバ20との間の通信速度が遅い場合、コンテンツサーバ20の管理事業者はアプリケーションを登録アプリケーション領域52Rに格納することを依頼するメリットが大きい。一方、ア

10 プリケーション本体を登録アプリケーション領域52Rに格納せず、移動体端末11から管理サーバ16に対しアプリケーションの配信要求がある毎にアプリケーション本体をコンテンツサーバ20から管理サーバ16に送信するようにすると、コンテンツサーバ20は各移動体端末11に応じたアプリケーションの配信を行うことが可能となる。例えば、コンテンツサーバ20は同じアプリケーション

15 に関して、各移動体端末11に対し個別のアクセスキーを設定して、正しい移動体端末11のユーザ以外の者によるそのアプリケーションの利用を禁止することができる。

コンテンツサーバ20-1が、あるアプリケーションの格納を管理サーバ16に依頼する際の処理を、図10および図11のフロー図を用いて説明する。まず、

20 コンテンツサーバ20-1は管理サーバ16に対し、アプリケーションの格納依頼を送信する(ステップS101)。この格納依頼にはアプリケーションの識別番号が含まれている。

管理サーバ16はアプリケーションの格納依頼を受信すると、格納依頼に含まれている識別番号を用いて、登録アプリケーション領域52Rのデータを読み出し、対象のアプリケーションに信頼度が与えられていることを確認する。対象の

25 アプリケーションに信頼度が与えられていることが確認できた場合、管理サーバ16はコンテンツサーバ20-1に対し、格納依頼の受諾通知を送信する(ステップS102)。

コンテンツサーバ20-1は格納依頼の受諾通知を受信すると、認証サーバ1

7に対し、管理サーバ16の公開鍵「PK-MS」の送信要求を行う（ステップS103）。認証サーバ17はこの公開鍵の送信要求に応じ、コンテンツサーバ20-1に対し「PK-MS」を送信する（ステップS104）。

コンテンツサーバ20-1は「PK-MS」を受信すると、アプリケーションを「PK-MS」を用いて暗号化する（ステップS105）。この暗号化処理により、アプリケーションがコンテンツサーバ20-1から管理サーバ16に送信される際、第三者がこれを傍受しても内容を解読することができず、アプリケーションが第三者により不正に使用されることが防がれる。

続いて、コンテンツサーバ20-1はコンテンツサーバ20-1の秘密鍵「SK-CS-1」を用いて、既に暗号化されているアプリケーションをさらに暗号化する（ステップS106）。この暗号化処理により、管理サーバ16はこのアプリケーションが間違いなくコンテンツサーバ20-1から送信されたものであることを確認することができる。すなわち、この暗号化処理は管理サーバ16がアプリケーションの送信元を確認するための証明書の役割を果たす。

15     コンテンツサーバ20-1は二重に暗号化されたアプリケーションを管理サーバ16に対し送信する（ステップS107）。

管理サーバ16は二重に暗号化されたアプリケーションを受信すると、管理サーバ16の暗号鍵格納部51のデータを読み出し、コンテンツサーバ20-1の公開鍵「PK-CS-1」が登録されているかどうかを確認する。管理サーバ16は、「PK-CS-1」が暗号鍵格納部51に登録されていない場合、認証サーバ17に対し「PK-CS-1」の送信要求を行う（ステップS108）。認証サーバ17はこの公開鍵の送信要求に応じ、管理サーバ16に対し「PK-CS-1」を送信する（ステップS109）。管理サーバ16は、「PK-CS-1」が暗号鍵格納部51に登録されている場合、改めて「PK-CS-1」を取得する必要はないので、ステップS108およびステップS109は行わず、次のステップS110に進む。

続いて、管理サーバ16は、二重に暗号化されたアプリケーションを「PK-CS-1」を用いて復号化する（ステップS110）。ここでアプリケーションの復号化に失敗した場合、管理サーバ16の受信したアプリケーションは送信途中

に改竄が行われたか、何らかの理由で破損しているか、コンテンツサーバ20-1以外のサーバから送信されたものであるのか、管理サーバ16はこのアプリケーションの格納処理を中止し、コンテンツサーバ20-1に正しいアプリケーションの再送要求を行う。一方、「PK-CS-1」を用いたアプリケーションの復号化が成功した場合、アプリケーションはコンテンツサーバ20-1から問題なく送信されたことが確認されるので、管理サーバ16は続いて、このアプリケーションを管理サーバ16の秘密鍵「SK-MS」を用いて復号化する（ステップS111）。管理サーバ16は上記の処理により、平文となったアプリケーションを取得できるので、その内容にコンテンツサーバ20-1による改竄等が行われていないことを確認できる。

なお、上記の処理のうち、ステップS103からステップS111までの一連の処理は、以下の説明において「管理サーバへのアプリケーション送信処理1」と呼ぶ。

管理サーバ16は、ステップS111の処理を終えると、アプリケーションそのアプリケーションを登録アプリケーション領域52Rに格納し（ステップS112）、コンテンツサーバ20-1に対し格納処理の完了通知を送信する（ステップS113）。

#### [1. 2. 2] アプリケーションの購入

アプリケーションの配信は、移動体端末11のユーザがアプリケーションを購入することにより可能となる。移動体端末11のユーザが希望するアプリケーションを購入する方法としては、管理サーバ16によって公開されているアプリケーションを購入する方法と、コンテンツサーバ20内のホームページ等を介して、移動体端末11のユーザがコンテンツサーバ20の管理事業者と直接購入契約を結ぶ方法がある。さらに、移動体端末11のユーザがコンテンツサーバ20の管理事業者と直接購入契約を結ぶ方法には、「1」以上の信頼度を与えられたアプリケーションを購入する場合と、信頼度が「0」であるアプリケーションを購入する場合がある。以下、それぞれの場合について、購入処理の流れを説明する。

[1. 2. 2. 1] 管理サーバにおいて公開されているアプリケーションの購入  
移動体端末11のユーザが管理サーバ16において公開されているアプリケー

ションを購入する場合の例として、移動体端末11-1のユーザが管理サーバ16を介してコンテンツサーバ20-1が配信元であるアプリケーションを購入する場合の処理を図12および図13および図14および図15を用いて説明する。

移動体端末11-1のユーザは、移動体端末11-1のアプリボタン23を押下して、画面D11に示すアプリケーションメニューを表示させる。続いて、移動体端末11-1のユーザは、操作部22のボタン「1」を押下して「1. アプリケーションの新規購入」を選択する。ボタン「1」が押下されると、移動体端末11-1は管理サーバ16に対し、アプリケーション情報一覧の送信要求を行う（ステップS201）。

10 管理サーバ16はアプリケーション情報一覧の送信要求を受信すると、登録アプリケーション領域52Rのデータを読み出し、公開に関する項目が「Yes」であり、かつユーザ情報格納部53-1に登録されていないアプリケーションの情報を抽出する。続いて、管理サーバ16は抽出された情報から、アプリケーションの識別番号、名称、機能、利用料金、料金徴収の代行の別、配信元のコンテンツサーバ20内の所定のホームページのURL等の情報を、アプリケーション情報一覧として移動体端末11-1に送信する（ステップS202）。

移動体端末11-1はアプリケーション情報一覧を受信すると、画面D12を表示させる。これに対し、移動体端末11-1のユーザは購入希望のアプリケーションに対応する番号のボタンを押下する。例えばユーザが画面D12においてボタン「1」を押下すると、「スケジュール管理 Ver. 2」が選択され、移動体端末11-1はディスプレイ部21に画面D13を表示する。画面D13には指定されたアプリケーションの機能に関する情報および利用料金が示されており、ユーザはこれらの情報に基づきこのアプリケーションの購入の判断を行う。

25 移動体端末11-1のユーザが画面D13においてアプリケーションの購入を決定し、ボタン「9」を押下すると、移動体端末11-1は指定されたアプリケーションの識別番号を管理サーバ16に送信する（ステップS203）。その後、移動体端末11-1はディスプレイ部21に画面D14を表示させる。

管理サーバ16はアプリケーションの識別番号を受信すると、登録アプリケーション領域52Rのデータを読み出し、対応するアプリケーションの保管場所を

確認する（ステップS 2 0 4）。

ここで指定されたアプリケーション本体が登録アプリケーション領域5 2 Rに格納されていない場合、管理サーバ1 6は登録アプリケーション領域5 2 Rのデータよりアプリケーションの保管場所情報としてコンテンツサーバ2 0 - 1内のURLを取得し、コンテンツサーバ2 0 - 1に対しアプリケーションの送信要求を送信する（ステップS 2 0 5）。

コンテンツサーバ2 0 - 1はアプリケーションの送信要求を受信すると、前述の「管理サーバへのアプリケーション送信処理1」を開始し、管理サーバ1 6、認証サーバ1 7、およびコンテンツサーバ2 0 - 1の間において図1 0および図1 1におけるステップS 1 0 3からステップS 1 1 1までの処理と同様の処理が行われる。その結果、管理サーバ1 6は該当するアプリケーションを取得する（ステップS 2 0 6）。

管理サーバ1 6は取得したアプリケーションに保管番号を与え、その保管番号と共にアプリケーションを一時保管アプリケーション領域5 2 Tに格納する（ステップS 2 0 7）。この保管番号は管理サーバ1 6が取得したアプリケーションを一時保管アプリケーション領域5 2 Tにおいて識別するためのものであり、同じ内容のアプリケーションであっても配信先の移動体端末が異なると異なる保管番号となる。

一方、移動体端末1 1 - 1により指定されたアプリケーションが管理サーバ1 6の登録アプリケーション領域5 2 Rに格納されている場合、管理サーバ1 6は既にアプリケーションを取得しているため、上記のステップS 2 0 5からステップS 2 0 7までの処理は行わず、次のステップS 2 0 8の処理に進む。

続いて、管理サーバ1 6はユーザ情報格納部5 3 - 1における配信可能アプリケーション領域5 3 Bにコンテンツサーバ2 0 - 1から取得したアプリケーションに関する情報、すなわちアプリケーションの識別番号、信頼度等を登録する（ステップS 2 0 8）。この登録処理により、移動体端末1 1 - 1のユーザは希望する時にこの既登録のアプリケーションを移動体端末1 1 - 1にダウンロードすることが可能となる。なお、この登録処理において、アクティベーションに関する項目に関しては、この時点ではまだコンテンツサーバ2 0 - 1から取得したアプリ

ケーションは移動体端末 11-1 にダウンロードされておらず、従ってアクティベーション処理も行われていないので、「No」が登録される。さらに、登録されるアプリケーションが一時保管アプリケーション領域 52T に格納されている場合には、配信可能アプリケーション領域 53B には保管番号も登録される。この登録処理が完了すると、管理サーバ 16 は移動体端末 11-1 に対し、アプリケーション購入処理の完了通知を送信する（ステップ S209）。

移動体端末 11-1 はアプリケーション購入処理の完了通知を受信すると、画面 D15 もしくは画面 D16 を表示する。画面 D15 は、新たに購入されたアプリケーションの利用に関し、料金徴収の代行依頼が行われている場合に表示される画面の例であり、移動体端末 11-1 のユーザに対し利用料金が通信料金と共に請求されることが通知される。一方、画面 D16 は、料金徴収の代行依頼が行われていない場合に表示される画面の例であり、移動体端末 11-1 のユーザに対し利用料金の支払手続を別途行うよう連絡がなされる。画面 D16 において、移動体端末 11-1 のユーザはボタン「0」を押下して、コンテンツサーバ 20-1 の管理事業者の運営する所定のホームページに移動し、そのホームページにおいて、購入したアプリケーションの料金支払に関する手続を行うことができる。

移動体端末 11-1 のユーザが、画面 D15 もしくは画面 D16 においてボタン「9」を押下してアプリケーションの新規購入の処理を終了すると、移動体端末 11-1 はディスプレイ部 21 に画面 D17 を表示する。画面 D17 は移動体端末 11-1 の通常の画面であるが、上部に「α」が表示されている。この「α」の表示は、移動体端末 11-1 のユーザに対し、新たにダウンロードが可能となったアプリケーションがあることを知らせるための表示である。なお、移動体端末 11-1 のユーザに対し、新たにダウンロードが可能となったアプリケーションがあることを知らせるための方法は「α」の表示に限られず、他の文字や画像の表示、および音や振動による通知であってもよい。

一方、ステップ S209 においてアプリケーション購入処理の完了通知を行った管理サーバ 16 は、続いてコンテンツサーバ 20-1 に対し移動体端末 11-1 によってアプリケーションの購入が行われたことを通知する（ステップ S210）。また、新たに移動体端末 11-1 によって購入処理が行われたアプリケーシ

ョンの料金徴収の代行依頼がなされている場合には、管理サーバ16は購入されたアプリケーションの識別番号、移動体端末11-1の識別番号、購入日時等の情報を課金管理サーバに送信する（ステップS211）。

【1.2.2.2】「1」以上の信頼度を与えられ、かつ公開されていないアプリ

#### 5 ケーションの購入

移動体端末11のユーザが、「1」以上の信頼度を与えられているが、管理サーバ16において公開されていないアプリケーションを購入する場合の例として、移動体端末11-1のユーザが、コンテンツサーバ20-1が配信元であるアプリケーションを購入する場合の処理を図16および図17を用いて説明する。

- 10 移動体端末11-1のユーザが、管理サーバ16において公開されていないアプリケーションを購入する場合、移動体端末11-1のユーザは、例えば移動体端末11-1を用いてコンテンツサーバ20-1内のホームページを開き、そのホームページにおいて目的のアプリケーションの購入申請を行う（ステップS301）。その際、必要であれば、移動体端末11-1のユーザは購入するアプリケーションの利用料金の支払手続も行うものとする。

- 15 コンテンツサーバ20-1は移動体端末11-1の購入申請の内容が所定の条件を満たしていることを確認した後、移動体端末11-1に対しアプリケーションの購入承諾通知を送信する（ステップS302）。この購入承諾通知にはアプリケーションの識別番号が含まれている。なお、コンテンツサーバ20-1は購入承諾通知を送信する際、購入承諾を行った移動体端末11-1の識別番号を記録する。

- 20 移動体端末11-1は、アプリケーションの購入承諾通知を受信すると、管理サーバ16に対し購入したアプリケーション情報の登録要求を送信する（ステップS303）。この登録要求には、新たに購入されたアプリケーションの識別番号が含まれている。

- 25 管理サーバ16は、移動体端末11-1から購入アプリケーション情報の登録要求を受信すると、登録アプリケーション領域52Rのデータを読み出し、登録要求のされたアプリケーションの識別番号からそのアプリケーションの配信元情報としてコンテンツサーバ20-1内のURLを取得する。続いて、管理サーバ



16はそのURLを用いて、コンテンツサーバ20-1に対し、移動体端末11-1に対する購入アプリケーション情報の登録を行ってよいかどうかを確認するための登録許可を要求する(ステップS304)。この登録許可の要求には、移動体端末11-1の識別番号が含まれている。

- 5     コンテンツサーバ20-1は管理サーバ16よりアプリケーション情報の登録許可の要求を受信すると、管理サーバ16がアプリケーション情報を登録しようとしている移動体端末の識別番号が、ステップS302においてアプリケーションの購入承諾を行った移動体端末の識別番号と一致することを確認する。コンテンツサーバ20-1は、それらの識別番号が一致すると、管理サーバ16に対し
- 10    アプリケーション情報の登録許可を通知する(ステップS305)。

管理サーバ16はコンテンツサーバ20-1よりアプリケーション情報の登録許可を受信すると、登録アプリケーション領域52Rのデータを読み出し、移動体端末11-1から登録要求のあったアプリケーションの保管場所を確認する(ステップS306)。

- 15    ステップS306において、登録要求のあったアプリケーション本体が登録アプリケーション領域52Rに格納されていない場合、管理サーバ16は登録アプリケーション領域52Rの保管場所に関する情報を用いて、コンテンツサーバ20-1に対し対応するアプリケーションの送信要求を送信する(ステップS307)。コンテンツサーバ20-1はアプリケーションの送信要求を受信すると、前
- 20    述の「管理サーバへのアプリケーション送信処理1」を開始し、管理サーバ16、認証サーバ17、およびコンテンツサーバ20-1の間において図10および図11におけるステップS103からステップS111までの処理と同様の処理が行われる。その結果、管理サーバ16は該当するアプリケーションを取得する(ステップS308)。管理サーバ16は取得したアプリケーションに保管番号を与え、
- 25    その保管番号と共にアプリケーションを一時保管アプリケーション領域52Tに格納する(ステップS309)。

一方、移動体端末11-1により登録要求のあったアプリケーションが登録アプリケーション領域52Rに格納されている場合、管理サーバ16は上記のステップS307からステップS309までの処理を行わず、次のステップS310

の処理に進む。

- 続いて、管理サーバ16はユーザ情報格納部53-1における配信可能アプリケーション領域53Bに、移動体端末11-1により登録要求のあったアプリケーションの情報、すなわちアプリケーションの識別番号、信頼度等を登録する（ステップS310）。なお、アクティベーションに関する項目については、まだアクティベーション処理が行われていないため、「N0」が登録される。また、アプリケーションが一時保管アプリケーション領域52Tに格納されている場合、配信可能アプリケーション領域53Bには保管番号も登録される。この登録処理により、移動体端末11-1のユーザは希望する時に新たに登録されたアプリケーションを移動体端末11-1にダウンロードすることが可能となる。従って、管理サーバ16は移動体端末11-1に対し、アプリケーション購入処理の完了通知を送信する（ステップS311）。

- 移動体端末11-1は、アプリケーション購入処理の完了通知を受信すると、ディスプレイ部21に「α」を表示し、購入されたアプリケーションが管理サーバ16よりダウンロード可能となったことをユーザに知らせる。

ここで、コンテンツサーバ20-1により管理サーバ16に対して、新たに登録が行われたアプリケーションの料金徴収の代行依頼がされている場合には、管理サーバ16はアプリケーションの識別番号、移動体端末11-1の識別番号、購入日時等の情報を課金管理サーバに送信する（ステップS312）。

- 20 [1. 2. 2. 3] 信頼度が「0」であるアプリケーションの購入

- 移動体端末11のユーザが、信頼度が「0」であるアプリケーションを購入する場合の例として、移動体端末11-1のユーザがコンテンツサーバ20-1が配信元であるアプリケーションを購入する場合の処理を図18、図19、および図20を用いて説明する。以下の処理は図16および図17を用いて説明したステップS301以下の処理と類似しているが、「1」以上の信頼度を与えられていないため、管理サーバ16はアプリケーションの内容を平文として取得する必要はない。従って、アプリケーションがコンテンツサーバ20-1から管理サーバ16に送信される際、アプリケーションは管理サーバ16の公開鍵ではなく、配信先の移動体端末11-1の公開鍵で暗号化される。その結果、移動体端末11

ー 1 のユーザ以外がアプリケーションの送信を傍受してもその内容を解読できないため、アプリケーションの不正使用が防止されるとともに、その内容の秘匿性が確保される。

- 5       まず、移動体端末 11-1 のユーザは、例えば移動体端末 11-1 を用いてコンテンツサーバ 20-1 内のホームページを開き、そのホームページにおいて目的のアプリケーションの購入を申請する（ステップ S 401）。その際、移動体端末 11-1 のユーザは購入するアプリケーションの利用料金の支払手続も行うものとする。

- 10       コンテンツサーバ 20-1 は移動体端末 11-1 の購入申請の内容が一定の条件を満たしていることを確認した後、移動体端末 11-1 に対しアプリケーションの購入承諾通知を送信する（ステップ S 402）。この購入承諾通知にはアプリケーションの識別番号が含まれている。また、コンテンツサーバ 20-1 は購入承諾通知を送信する際、購入承諾を行った移動体端末 11-1 の識別番号を記録する。

- 15       移動体端末 11-1 は、アプリケーションの購入承諾通知を受信すると、管理サーバ 16 に対し、新たに購入したアプリケーション情報の登録要求を送信する（ステップ S 403）。この登録要求には、アプリケーションの識別番号およびアプリケーションの保管場所情報としてコンテンツサーバ 20-1 内の URL が含まれている。

- 20       管理サーバ 16 は、移動体端末 11-1 からアプリケーション情報の登録要求を受信すると、コンテンツサーバ 20-1 に対し、アプリケーションの送信要求を行う（ステップ S 404）。この送信要求には、移動体端末 11-1 の識別番号が含まれている。

- 25       コンテンツサーバ 20-1 は管理サーバ 16 よりアプリケーションの送信要求を受信すると、送信要求を行っている移動体端末の識別番号が、ステップ S 402 においてアプリケーションの購入承諾を行った移動体端末の識別番号と一致するかどうかを確認する。これらの識別番号が一致する場合、コンテンツサーバ 20-1 は、認証サーバ 17 に対し移動体端末 11-1 の公開鍵「PK-MT-1」の送信を要求する（ステップ S 405）。認証サーバ 17 は「PK-MT-1」の

送信要求を受信すると、コンテンツサーバ20-1に対し「PK-MT-1」を送信する（ステップS406）。

コンテンツサーバ20-1は「PK-MT-1」を受信すると、送信要求のされたアプリケーションを「PK-MT-1」を用いて暗号化する（ステップS407）。

続いて、コンテンツサーバ20-1はコンテンツサーバ20-1の秘密鍵「SK-CS-1」を用いて、既に暗号化されているアプリケーションをさらに暗号化する（ステップS408）。この暗号化処理により、管理サーバ16はこのアプリケーションが間違いなくコンテンツサーバ20-1から送信されたものであることを確認することができる。

コンテンツサーバ20-1は二重に暗号化されたアプリケーションを管理サーバ16に対し送信する（ステップS409）。

管理サーバ16は二重に暗号化されたアプリケーションを受信すると、管理サーバ16の暗号鍵格納部51のデータを読み出し、コンテンツサーバ20-1の公開鍵「PK-CS-1」が登録されているかどうかを確認する。管理サーバ16は、「PK-CS-1」が暗号鍵格納部51に登録されていない場合、認証サーバ17に対し「PK-CS-1」の送信要求を行う（ステップS410）。認証サーバ17はこの公開鍵の送信要求に応じ、管理サーバ16に対し「PK-CS-1」を送信する（ステップS411）。管理サーバ16は、「PK-CS-1」が暗号鍵格納部51に登録されている場合、改めて「PK-CS-1」を取得する必要はないので、ステップS410およびステップS411は行わず、次のステップS412に進む。

続いて、管理サーバ16は、二重に暗号化されたアプリケーションを「PK-CS-1」を用いて復号化する（ステップS412）。ここでアプリケーションの復号化に失敗した場合、管理サーバ16の受信したアプリケーションは送信途中に改竄が行われたか、何らかの理由で破損しているか、コンテンツサーバ20-1以外のサーバから送信されたものであるか、管理サーバ16はこのアプリケーションの格納処理を中止し、コンテンツサーバ20-1に正しいアプリケーションの再送要求を行う。一方、「PK-CS-1」を用いたアプリケーションの復

号化が成功した場合、アプリケーションはコンテンツサーバ20-1から問題なく送信されたことが確認される。

なお、以下の説明において、上記のステップS405からステップS412までの一連の処理を、「管理サーバへのアプリケーション送信処理2」と呼ぶ。

- 5       続いて、管理サーバ16はそのアプリケーションに保管番号を与え、その保管番号と共にアプリケーションを一時保管アプリケーション領域52Tに格納する（ステップS413）。なお、この場合、一時保管アプリケーション領域52Tに格納されるアプリケーションは移動体端末11-1の公開鍵「PK-MT-1」により暗号化されたままであり、管理サーバ16の管理事業者等から内容を解読
- 10      されることはない。

- 続いて、管理サーバ16は、登録アプリケーション領域52Rにアプリケーションの識別番号およびアプリケーションの保管場所情報としてコンテンツサーバ20-1内のURLを登録する（ステップS414）。この登録は、管理サーバ16が移動体端末11-1からの要求に応じ、同じアプリケーションを再度コンテンツサーバ20-1から取得する際に必要な情報の登録処理である。なお、この
- 15      アプリケーションに関する登録アプリケーション領域52Rにおける信頼度は「0」、公開および料金徴収に関する項目は空欄（「-」）となる。

- 次に、管理サーバ16はユーザ情報格納部53-1における配信可能アプリケーション領域53Bに、移動体端末11-1により登録要求のあったアプリケーション情報、すなわちアプリケーションの識別番号、保管番号等を登録する（ステップS415）。なお、アクティベーションに関する項目については、「No」が登録され、信頼度に関する項目については、「0」が登録される。この登録処理により、移動体端末11-1のユーザは希望する時に新たに登録されたアプリケーションを移動体端末11-1にダウンロードすることが可能となる。管理サーバ16はこの登録処理を完了すると、移動体端末11-1に対し、アプリケーションの購入処理の完了通知を送信する（ステップS416）。
- 20
- 25

          移動体端末11-1は、アプリケーション購入処理の完了通知を受信すると、ディスプレイ部21に「α」を表示し、購入されたアプリケーションが管理サーバ16よりダウンロード可能となったことをユーザに知らせる。

## [1. 2. 3] 移動体端末によるアプリケーションのダウンロード

移動体端末 11 のユーザはアプリケーションを購入した後、購入したアプリケーションをダウンロードする必要がある。以下、アプリケーションのダウンロードの処理を、移動体端末 11-1 を例として図 21 および図 22 および図 23、  
5 図 24、および図 25 を用いて説明する。

移動体端末 11-1 のユーザは、まず移動体端末 11-1 のアプリボタン 23 を押下して、画面 D21 のアプリケーションメニューを表示させる。画面 D21 において、移動体端末 11-1 のユーザは、操作部 22 のボタン「2」を押下して「2. アプリケーションのダウンロード」を選択する。ボタン「2」が押下さ  
10 れると、移動体端末 11-1 は管理サーバ 16 に対し、ダウンロードの可能なアプリケーション情報一覧の送信要求を行う（ステップ S501）。

管理サーバ 16 はアプリケーション情報一覧の送信要求を受信すると、ユーザ情報格納部 53-1 の配信可能アプリケーション領域 53B に登録されているアプリケーションの名称を、アプリケーションの識別番号と共にアプリケーション  
15 情報一覧として移動体端末 11-1 に送信する（ステップ S502）。

移動体端末 11-1 はアプリケーション情報一覧を受信すると、画面 D22 を表示させる。これに対し、移動体端末 11-1 のユーザは対応する番号のボタンを押下することにより、ダウンロードするアプリケーションの指定を行う。例えばユーザが画面 D22 においてボタン「1」を押下すると、「スケジュール管理  
20 Ver. 2」という名称のアプリケーションが選択される。移動体端末 11-1 のユーザによるボタン操作によりアプリケーションが指定されると、移動体端末 11-1 は管理サーバ 16 に対し、指定されたアプリケーションの識別番号を送信する（ステップ S503）。

管理サーバ 16 は指定されたアプリケーションの識別番号を受信すると、配信  
25 可能アプリケーション領域 53B のデータを読み出し、指定されたアプリケーションが信頼度の与えられたものであるか否かを確認する。続いて、管理サーバ 16 は既配信アプリケーション領域 53A のデータを読み出し、移動体端末 11-1 のメモリ 12 において、指定されたアプリケーションを書き込むために必要な空き容量があるかどうかを確認する（ステップ S504）。その際、指定されたア

アプリケーションに信頼度が与えられている場合は、管理エリア 40 に空き容量があるかどうかを確認される。一方、指定されたアプリケーションに信頼度が与えられていない場合は、フリーエリア 41 に空き容量があるかどうかを確認される。

- 5     ステップ S 504 において、移動体端末 11-1 のメモリ 12 に指定されたアプリケーションを書き込むための空き容量が十分でない場合、管理サーバ 16 は移動体端末 11-1 に対し、メモリ 12 上から削除すべきアプリケーションの指定要求を送信する（ステップ S 505）。この指定要求には、ダウンロードの指定のされたアプリケーションが信頼度の与えられたものであるか否かの情報が含まれている。移動体端末 11-1 はこの指定要求を受信すると、画面 D 23 をディスプレイ部 21 に表示させる。移動体端末 11-1 のユーザがこの画面に対しボタン「9」を押下して実行の指示を行うと、移動体端末 11-1 はさらに画面 D 24 をディスプレイ部 21 に表示させる。ダウンロードの指定のされたアプリケーションが信頼度の与えられたものである場合、画面 D 24 には管理エリア 40 に書き込まれているアプリケーションの名称が表示され、ダウンロードの指定のされたアプリケーションが信頼度の与えられていないものである場合、画面 D 24 にはフリーエリア 41 に書き込まれているアプリケーションの名称が表示される。この画面において、移動体端末 11-1 のユーザは対応するボタンを押下することにより、メモリ 12 から削除するアプリケーションを指定する。移動体端末 11-1 は指定されたアプリケーションの識別番号を管理サーバ 16 に送信する（ステップ S 506）。なお、ステップ S 506 の処理の後、移動体端末 11-1 はディスプレイ部 21 に画面 D 25 を表示させる。

- 25     一方、ステップ S 504 において、指定されたアプリケーションを書き込むための空き容量が移動体端末 11-1 のメモリ 12 に十分ある場合、ステップ S 505 およびステップ S 506 の処理は行われず、管理サーバ 16 は次のステップ S 507 の処理に進む。また、移動体端末 11-1 はディスプレイ部 21 に画面 D 25 を表示させる。

続いて、管理サーバ 16 は配信可能アプリケーション領域 53B のデータを読み出し、移動体端末 11-1 によりダウンロードの指定のされたアプリケーションがアプリケーション情報格納部 52 に格納されているか否かを確認する（ステ

ップS 5 0 7)。図7を用いて、アプリケーションがアプリケーション情報格納部5 2に格納されている場合とそうでない場合の例を示す。

移動体端末1 1-1によりダウンロードの指定のされたアプリケーションの識別番号が「AP-4 1 2 5」であった場合、図7の例によれば対応するアプリケーションの保管場所が「T-7 8 5 1」であることが分かる。これは目的のアプリケーションが一時保管アプリケーション領域5 2 Tに格納されていることを意味する。また、移動体端末1 1-1によりダウンロードの指定のされたアプリケーションの識別番号が「AP-4 5 1 3」であった場合、図7の例によれば対応するアプリケーションの保管場所のデータが与えられていない。これは対応するアプリケーションが登録アプリケーション領域5 2 Rに格納依頼がなされているアプリケーションであることを意味する。従って、目的のアプリケーションは登録アプリケーション領域5 2 Rに格納されている。

これらに対し、移動体端末1 1-1によりダウンロードの指定のされたアプリケーションの識別番号が「AP-3 0 2 1」であった場合、図7の例によれば対応するアプリケーションの保管場所が「削除済み」となっている。これは対応するアプリケーションが、一時保管アプリケーション領域5 2 Tにも、登録アプリケーション領域5 2 Rにも格納されていないことを意味する。このように、配信可能アプリケーション領域5 3 Bに登録されているアプリケーションが、アプリケーション情報格納部5 2に格納されていない状況が発生する理由は、以下のステップS 5 2 3において説明するように、登録アプリケーション領域5 2 Rにおける格納依頼のされていないアプリケーションであって、一度ダウンロードされたアプリケーションに関しては、ダウンロードされた時点で一時保管アプリケーション領域5 2 Tに格納されていたアプリケーションが削除されるためである。

上記の識別番号「AP-3 0 2 1」のアプリケーションの例のように、ステップS 5 0 7において、ダウンロードの指定のされたアプリケーションがアプリケーション情報格納部5 2に格納されていない場合、管理サーバ1 6は登録アプリケーション領域5 2 Rのデータを読み出し、ダウンロードの指定のされたアプリケーションの識別番号に対応する保管場所としてコンテンツサーバ2 0-1内のURLを取得し、コンテンツサーバ2 0-1に対しアプリケーションの送信要求



を送信する（ステップS 5 0 8）。

ダウンロードの指定のされたアプリケーションが信頼度の与えられたアプリケーションである場合、ステップS 5 0 8に続いて、コンテンツサーバ2 0、認証サーバ1 7、および管理サーバ1 6の間で、「管理サーバへのアプリケーション送信処理1」と同様の処理が行われる。一方、ダウンロードの指定のされたアプリケーションが信頼度の与えられていないアプリケーションである場合、ステップS 5 0 8に続いて、コンテンツサーバ2 0、認証サーバ1 7、および管理サーバ1 6の間で、「管理サーバへのアプリケーション送信処理2」と同様の処理が行われる。その結果、管理サーバ1 6は該当するアプリケーションを取得する（ステップS 5 0 9）。

続いて、管理サーバ1 6はステップS 5 0 9の処理により取得したアプリケーションを、一時保管アプリケーション領域5 2 Tに格納する（ステップS 5 1 0）。

これに対して、ステップS 5 0 7において、上記の識別番号が「AP-4 1 2 5」もしくは「AP-4 5 1 3」のアプリケーションの例のように、ダウンロードの指定のされたアプリケーションがアプリケーション情報格納部5 2に格納されている場合、管理サーバ1 6はステップS 5 0 8からステップS 5 1 0までの処理は行わず、次のステップS 5 1 1に進む。

続いて、管理サーバ1 6はアプリケーション情報格納部5 2に格納されているダウンロードの指定のされたアプリケーションが、暗号化されているかどうかを確認する（ステップS 5 1 1）。ダウンロードの指定のされたアプリケーションが信頼度の与えられたアプリケーションである場合、アプリケーション情報格納部5 2には平文のアプリケーションが格納されている。一方、ダウンロードの指定のされたアプリケーションが信頼度の与えられていないアプリケーションである場合、アプリケーション情報格納部5 2には移動体端末1 1-1の公開鍵を用いて暗号化されたアプリケーションが格納されている。

ステップS 5 1 1において、アプリケーション情報格納部5 2に格納されているダウンロードの指定のされたアプリケーションが暗号化されていない場合、管理サーバ1 6は、認証サーバ1 7に対し、移動体端末1 1-1の公開鍵「PK-MT-1」の送信要求を行う（ステップS 5 1 2）。認証サーバ1 7はこの公開鍵

の送信要求に応じ、管理サーバ16に対し「PK-MT-1」を送信する（ステップS513）。

管理サーバ16は「PK-MT-1」を受信すると、移動体端末11-1のメモリ12においてアプリケーションを書き込むべき場所を示す情報をアプリケーションに添付する。また、アプリケーションに信頼度が与えられている場合、管理サーバ16はアプリケーションにその信頼度も添付する。その後、管理サーバ16はアプリケーションを「PK-MT-1」を用いて暗号化する（ステップS514）。この暗号化処理により、アプリケーションが管理サーバ16から移動体端末11-1に送信される際、第3者がこれを傍受しても、移動体端末11-1以外はこれを復号化することができず、アプリケーションが第3者により不正に使用されることが防がれる。

これに対し、ステップS511において、アプリケーション情報格納部52に格納されているダウンロードの指定のされたアプリケーションが暗号化されている場合、管理サーバ16は上記のステップS512からステップS514までの処理を行わず、次のステップS515に進む。

続いて、管理サーバ16は管理サーバ16の秘密鍵「SK-MS」を用いて、既に暗号化されているアプリケーションをさらに暗号化する（ステップS515）。この暗号化処理により、移動体端末11-1はこのアプリケーションが間違いなく管理サーバ16から送信されたものであることを確認することができる。すなわち、この暗号化処理は移動体端末11-1がアプリケーションの出所を確認するための証明書の役割を果たす。

管理サーバ16は二重に暗号化されたアプリケーションを、移動体端末11-1に対し送信する（ステップS516）。

移動体端末11-1は二重に暗号化されたアプリケーションを受信すると、認証サーバ17に対し管理サーバ16の公開鍵「PK-MS」の送信要求を行う（ステップS517）。認証サーバ17はこの公開鍵の送信要求に応じ、移動体端末11-1に対し「PK-MS」を送信する（ステップS518）。

移動体端末11-1は「PK-MS」を受信すると、二重に暗号化されたアプリケーションをまず「PK-MS」を用いて復号化する（ステップS519）。こ

ここで復号化に失敗した場合、移動体端末 11-1 の受信したアプリケーションは途中で改竄が行われたか、何らかの理由で破損しているか、管理サーバ 16 以外のサーバから送信されたものであるので、移動体端末 11-1 は管理サーバ 16 に正しいアプリケーションの再送要求を行う。一方、「PK-MS」を用いた復号化が成功した場合、アプリケーションは管理サーバ 16 から問題なく送信されたものであると確認されるので、移動体端末 11-1 は続いてこのアプリケーションを移動体端末 11-1 の秘密鍵「SK-MT-1」を用いて復号化する（ステップ S 5 2 0）。

移動体端末 11-1 は上記の処理により、平文となったアプリケーションを、  
10 移動体端末 11-1 のメモリ 12 においてアプリケーションを書き込むべき場所を示す情報とともに取得する。移動体端末 11-1 は、受信したアプリケーションを、書き込みべき場所に関する情報により指定されたメモリエリアのアプリケーション領域 40 A もしくはアプリケーション領域 41 A に書き込む（ステップ S 5 2 1）。ここで、受信したアプリケーションに信頼度が添付されている場合には、移動体端末 11-1 は、アプリケーションを書き込んだ管理エリア 40 における信頼情報領域 40 R に、信頼度を書き込む。この際、指定された領域にステップ S 5 0 6 において移動体端末 11-1 のユーザが削除を指定したアプリケーションがある場合には、そのアプリケーションは新たなアプリケーションで上書きされる。続いて、移動体端末 11-1 は管理サーバ 16 に対しアプリケーションの書き込み完了通知を送信する（ステップ S 5 2 2）。移動体端末 11-1 はステップ S 5 2 2 の処理を終えると、ディスプレイ部 21 に通常の画面である画面 D 2 6 を表示させる。

管理サーバ 16 はアプリケーションの書き込み完了通知を受信すると、ユーザ情報格納部 53 およびアプリケーション情報格納部 52 のデータの更新を行う  
25 （ステップ S 5 2 3）。具体的には、まず移動体端末 11 のメモリ 12 より削除されたアプリケーションがある場合、そのアプリケーションの情報を既配信アプリケーション領域 53 A から配信可能アプリケーション領域 53 B に移動する。次に、新たにメモリ 12 に書き込まれたアプリケーションの情報を、配信可能アプリケーション領域 53 B から既配信アプリケーション領域 53 A の対応する場所

に移動する。さらに、書き込まれたアプリケーションが一時保管アプリケーション領域 5 2 T に一時的に格納されていたアプリケーションである場合は、一時保管アプリケーション領域 5 2 T からそのアプリケーションを削除する。

[1. 2. 4] アプリケーションのアクティベーション

- 5     上記のように移動体端末 1 1 がアプリケーションをダウンロードしても、移動体端末 1 1 のユーザがそのアプリケーションを利用するにはアクティベーション処理を行う必要がある。

- 10     アクティベーション処理とは、管理サーバ 1 6 が、ダウンロードされたアプリケーションの利用許可通知を、移動体端末 1 1 のメモリコントローラ 3 5 に対し与える処理である。移動体端末 1 1 のメモリ 1 2 にダウンロードされたアプリケーションが、特にアプリケーションの利用期間に制限のないアプリケーションである場合には、アクティベーション処理はアプリケーションのダウンロード処理の後、引き続き実行される。しかしながら、アプリケーションの利用期間に制限のあるアプリケーションに関しては、アプリケーションのダウンロードの後、利用  
15     期間が開始されるまでの間はアクティベーション処理は行われず、利用開始期間が訪れた際、アクティベーション処理が行われる。

- 20     例えば、移動体端末 1 1 - 1 が 4 月 1 日より有効な定期乗車券の機能を持つアプリケーションを 3 月 1 5 日に購入し、そのアプリケーションを 3 月 2 0 日に移動体端末 1 1 - 1 にダウンロードした場合、3 月 2 0 日から 3 月 3 1 日までの間は、そのアプリケーションは移動体端末 1 1 - 1 のメモリ 1 2 に書き込まれているが、利用できない。3 月 3 1 日から 4 月 1 日に日付が変わる時点で、このアプリケーションに関するアクティベーション処理が行われ、移動体端末 1 1 - 1 のユーザは 4 月 1 日以降にこのアプリケーションを利用することができる。

- 25     ダウンロード処理とアクティベーション処理とを別個に行うことにより、移動体端末 1 1 のユーザは、アプリケーションの有効期限に拘束されことなく望む時間にアプリケーションをダウンロードすることができる。また、同じ利用開始日を持つアプリケーションを多くの移動体端末 1 1 が利用する必要がある場合、もし利用開始日にダウンロード処理を行う必要があれば、多くの人が一斉にそれらのアプリケーションをダウンロードするため、管理サーバ 1 6、コンテンツサ

サーバ20、および移動体端末11の間の通信経路において、データの輻輳を引き起こしやすい。しかしながら、アクティベーション処理におけるデータ通信量はダウンロード処理におけるデータ通信量と比較して極めて小さいため、上記のような場合において、各移動体端末11のユーザがダウンロード処理をアクティベーション処理に先んじて自由な時間に行っておくことにより、アプリケーションの利用開始日に通信経路におけるデータの輻輳の発生を抑制することができる。

5 以下にアクティベーション処理の流れを説明する。

アクティベーション処理が発生するのは、利用期間に制限のないアプリケーションが移動体端末11-1にダウンロードされた場合、既に移動体端末11-1

10 にダウンロードされているアプリケーションに対し利用開始の時期が訪れた場合、もしくはアプリケーションの配信元であるコンテンツサーバ20からアクティベーションの指示が管理サーバ16に対しなされた場合などである。以下に例として、移動体端末11-1の管理エリア40-1に書き込まれているアプリケーションに対し、アクティベーション処理が行われる場合の処理の流れを説明する。

15 まず、管理サーバ16は移動体端末11-1に対しアクティベーション命令を送信する。このアクティベーション命令には、メモリ12における対象のアプリケーションの特定情報として、管理エリア40-1の識別番号が含まれている。

移動体端末11-1の通信部34はアクティベーション命令を受信すると、その命令をメモリコントローラ35に送る。メモリコントローラ35は、このアクティベーション命令を受信するまでの間、管理エリア40-1のアプリケーション領域40A-1およびデータ領域40D-1内のアプリケーションやデータに

20 対する、移動体端末11-1の制御部31による利用要求を全て拒否する。従って、その間、移動体端末11-1のユーザは管理エリア40-1のアプリケーションを利用することができない。

25 これに対し、メモリコントローラ35がアクティベーション命令を受信した後は、管理エリア40-1のアプリケーション領域40A-1およびデータ領域40D-1内のアプリケーションやデータに対する、制御部31の利用要求を受信すると、メモリコントローラ35はまず、管理エリア40-1の信頼情報領域40R-1に書き込まれている信頼度を読み出す。続いて、メモリコントローラ3

5 は利用要求と共に制御部 31 から送信される、利用要求元のプログラムの信頼度と、信頼情報領域 40R-1 から読み出した信頼度とを比較する。そして、メモリコントローラ 35 は、利用要求元のプログラムの信頼度が信頼情報領域 40R-1 から読み出した信頼度より高い場合、もしくは 2 つの信頼度が等しい場合にのみ、利用要求に従った処理を行う。この信頼度を用いた制御処理については、既に移動体端末 11 の構成におけるメモリコントローラ 35 の機能説明において述べたとおりである。

管理サーバ 16 は、アクティベーション命令を移動体端末 11-1 に送信した後、ユーザ情報格納部 53-1 における既配信アプリケーション領域 53A のアクティベーションに関する項目を「Yes」に更新する。続いて、管理サーバ 16 は、登録アプリケーション領域 52R のデータを読み出し、アクティベーション処理の対象のアプリケーションの料金徴収に関する項目が「Yes」である場合には、アプリケーションの識別番号、移動体端末 11-1 の識別番号、アクティベーション処理のなされた日時等の情報を課金管理サーバに送信する。

15 一方、移動体端末 11-1 は新たにアクティベーション命令を受信した場合、ディスプレイ部 21 に「α」を表示させ、移動体端末 11-1 のユーザに新たなアプリケーションが利用可能となったことを知らせる（図 26、画面 D31）。なおこの「α」の文字は、先に説明したアプリケーション購入処理の完了通知と区別するために「β」等の他の文字や、図形、音、振動等の他の方法を用いてもよい。

以上がアクティベーション処理である。なお、移動体端末 11-1 のユーザがアクティベーション処理が行われたアプリケーションを起動する場合、まず移動体端末 11-1 のユーザは、アプリボタン 23 を押下し、アプリケーションメニューを表示させる（画面 D32）。続いて、移動体端末 11-1 のユーザはボタン  
25 「3」を押下することにより「3. アプリケーションの起動」を指定し、利用可能なアプリケーションの選択画面を表示させる（画面 D33）。アプリケーションの選択画面において、移動体端末 11-1 が例えばボタン「1」を押下し、「1. スケジュール管理 Ver. 2」を選択すると、選択されたアプリケーションが起動される（画面 D34）。

## [1. 2. 5] アプリケーションのディアクティベーション

移動体端末 11-1 において、既にアクティベーション処理が行われたアプリケーションに対し、その利用を一時的に停止させる必要が生じる場合がある。例えば、移動体端末 11-1 が紛失もしくは盗難に遭った場合には、移動体端末 11-1 のユーザの要求により、移動体端末 11-1 にダウンロードされている全てのアプリケーションの利用を禁止する必要がある。また、移動体端末 11-1 のユーザによりアプリケーションの利用料金が滞納された場合や移動体端末 11-1 のユーザによる利用条件違反があった場合、コンテンツサーバ 20-1 もしくは管理サーバ 16 の管理事業者の要求により、移動体端末 11-1 にダウンロードされている特定のアプリケーションに関し、利用を一時的に停止させる必要がある。

上記のような場合、ディアクティベーション処理が行われる。以下に例として、移動体端末 11-1 の管理エリア 40-1 に書き込まれているアプリケーションに対し、ディアクティベーション処理が行われる場合の処理の流れを説明する。

まず、管理サーバ 16 は移動体端末 11-1 に対しディアクティベーション命令を送信する。このディアクティベーション命令には、メモリ 12 における対象のアプリケーションの特定情報として、管理エリア 40-1 の識別番号が含まれている。

移動体端末 11-1 の通信部 34 はディアクティベーション命令を受信すると、その命令をメモリコントローラ 35 に送る。メモリコントローラ 35 は、このディアクティベーション命令を受信すると、それ以降、管理エリア 40-1 のアプリケーション領域 40A-1 およびデータ領域 40D-1 内のアプリケーションやデータに対する、移動体端末 11-1 の制御部 31 による利用要求を全て拒否する。従って、移動体端末 11-1 のユーザは管理エリア 40-1 のアプリケーションを利用することができなくなる。

管理サーバ 16 はディアクティベーション命令を移動体端末 11-1 に送信した後、ユーザ情報格納部 53-1 における既配信アプリケーション領域 53A のアクティベーションに関する項目を「No」に更新する。続いて、管理サーバ 16 は、登録アプリケーション領域 52R のデータを読み出し、ディアクティベ

ション処理の対象のアプリケーションの料金徴収に関する項目が「Yes」である場合には、アプリケーションの識別番号、移動体端末11-1の識別番号、ディアクティベーション処理のなされた日時等の情報を課金管理サーバに送信する。

- 以上がディアクティベーション処理である。移動体端末11-1はディアクティベーション命令を受信した場合、利用可能なアプリケーションの選択画面において該当するアプリケーションの名称を表示しなくなる。なお、一度ディアクティベーション処理のされたアプリケーションを再度利用したい場合には、既に説明したアクティベーション処理を行う。例えば、紛失していた移動体端末11-1が見つかったり、移動体端末11-1のユーザによるアプリケーションの利用料金の滞納が解消したりした際、再度アクティベーション処理が行われるが、その場合、既に移動体端末11-1のメモリ12にダウンロードされていたアプリケーションやそのアプリケーションが管理していたデータはディアクティベーション処理のされた時点の状態で、再度利用可能となる。

#### [1. 2. 6] アプリケーションの削除

- 15 移動体端末11-1において、アプリケーションの利用を完全に中止させる必要が生じる場合がある。例えば、移動体端末11-1のユーザがアプリケーションの購入契約を解約する場合、予め定められていたアプリケーションの利用可能期間が満了した場合、移動体端末11-1のユーザが深刻なアプリケーションの利用条件違反を行った場合などである。そのような場合、以下の削除処理によって、アプリケーションを移動体端末11-1のメモリ12から削除すると同時に、
- 20 ユーザ情報格納部53-1の配信可能アプリケーション領域53Bからも、削除対象のアプリケーションに関するデータを削除する。以下に例として、移動体端末11-1の管理エリア40-1に書き込まれているアプリケーションに対し、削除処理が行われる場合の処理の流れを説明する。

- 25 まず、管理サーバ16はユーザ情報格納部53-1の既配信アプリケーション領域53Aのデータを読み出し、削除の対象となるアプリケーションが移動体端末11-1のメモリ12に書き込まれているかどうかを確認する。

対象のアプリケーションが移動体端末11-1のメモリ12に書き込まれている場合、管理サーバ16は移動体端末11-1に対し削除命令を送信する。この



削除命令には、対象のアプリケーションの特定情報として、管理エリア 40-1 の識別番号が含まれている。移動体端末 11-1 の通信部 34 は削除命令を受信すると、その命令をメモリコントローラ 35 に送る。メモリコントローラ 35 は削除命令を受信すると、識別番号により指定された管理エリア 40-1 内のアプリケーションおよびデータを消去する。移動体端末 11-1 のメモリコントローラ 35 はこの消去処理を終えると、管理サーバ 16 に対し消去完了通知を送信する。管理サーバ 16 は消去完了通知を受信すると、ユーザ情報格納部 53-1 における既配信アプリケーション領域 53A から、該当するアプリケーションの情報を削除する。

- 10 一方、対象のアプリケーションが移動体端末 11-1 のメモリ 12 に書き込まれていない場合、管理サーバ 16 はユーザ情報格納部 53-1 における配信可能アプリケーション領域 53B から、該当するアプリケーションの情報を削除する。

- 続いて、管理サーバ 16 は登録アプリケーション領域 52R のデータを読み出し、対象のアプリケーションの料金徴収に関する項目が「Yes」である場合には、アプリケーションの識別番号、移動体端末 11-1 の識別番号、削除処理の  
15 なされた日時等の情報を課金管理サーバに送信する。

以上が削除処理である。この削除処理により、移動体端末 11-1 の利用可能なアプリケーションの選択画面およびダウンロード可能なアプリケーションの表示画面において、該当するアプリケーションの名称は表示されなくなる。

- 20 [1. 3] 信頼度を用いたアプリケーション間の関係

続いて、信頼度を用いたアプリケーション間の関係方法について、具体例を用いて説明する。

- 既に説明したように、移動体端末 11-1 のメモリ 12 には複数のアプリケーションが書き込まれるが、管理エリア 40 に書き込まれているアプリケーション  
25 に関しては、信頼情報領域 40R に、それぞれのアプリケーションに対して与えられている信頼度が、「1」から「5」までの数値で格納されている。信頼度はその数値が大きいほど信頼性が高いことを示し、信頼度が高いアプリケーションは信頼度が低いアプリケーションの機能や、信頼度が低いアプリケーションの管理するデータを利用することが可能であるが、信頼度が低いアプリケーションから

は信頼度の高いアプリケーションの機能や、信頼度が高いアプリケーションの管理するデータを利用することはできない。なお、移動体端末 11 の制御部 31 が管理し、制御用メモリ 32 に書き込まれている制御用プログラムに関しては、信頼度「5」が与えられている。一方、フリーエリア 41 に書き込まれているアプリケーションに関しては、信頼度は与えられておらず、フリーエリア 41 に書き込まれているアプリケーションと他のプログラムとの信頼度の比較を行う必要がある場合には、フリーエリア 41 に書き込まれているアプリケーションには信頼度として「0」が適用される。

[1. 3. 1] アプリケーション間の関係が許可されない場合

以下に説明する例は、信頼度が低いアプリケーションから信頼度が高いアプリケーションの機能の呼び出しおよびデータの利用を行うことができないことを示す例である。なお、以下の説明には図 27、図 28、図 29、図 30、および図 31 を用いる。

まず、移動体端末 11-1 の管理エリア 40-1 におけるアプリケーション領域 40A に、定期乗車券機能を持ったアプリケーション（以下、「定期券アプリケーション」と呼ぶ）が書き込まれており、アクティベーション処理がなされ利用可能となっている。定期券アプリケーションを用いると、移動体端末 11-1 のユーザは「a b c 鉄道」のホームページを開き、そのホームページにおいて時刻表を閲覧したり、定期乗車券の購入を行ったりすることができる。なお、定期乗車券を購入した場合、例えば移動体端末 11-1 が「a b c 鉄道」の改札機に近づくと、改札機より発信されている電波信号に応じて移動体端末 11-1 からは所定の信号が発信され、改札機がゲートを開くようになっており、移動体端末 11-1 自体が定期乗車券の役割をする。この定期券アプリケーションの信頼度は「3」である。

一方、管理エリア 40-2 におけるアプリケーション領域 40A には、代金決済機能を持ったアプリケーション（以下、「決済アプリケーション」と呼ぶ）が書き込まれており、アクティベーション処理がなされ利用可能となっている。決済アプリケーションを用いると、移動体端末 11-1 のユーザは「x x 銀行」のホームページを開き、そのホームページにおいて移動体端末 11-1 のユーザの保

有する口座から任意の口座に送金を行うことができる。この決済アプリケーションの信頼度は「5」である。

移動体端末11-1のユーザは、アプリボタン23を押下し、アプリケーションメニュー（画面D41）をディスプレイ部21に表示させる。続いて、ユーザは画面D41においてボタン「3」を押下し、起動するアプリケーションの選択画面（画面D42）を表示する。ユーザは画面D42においてボタン「1」を押下し、定期券アプリケーションを選択する。移動体端末11-1は定期券アプリケーションを起動し、定期券アプリケーションは「a b c 鉄道」のホームページを開く（画面D43）。

10 画面D43において、ユーザがボタン「3」を押下して「3. 定期乗車券購入」を選択すると、移動体端末11-1は画面D44を表示する。画面D44において、ユーザは購入する定期乗車券の利用区間および利用期間を操作部22を用いて入力し、ボタン「9」を押下して「a b c 鉄道」のホームページに対し、購入指示を送信する。

15 ここで、定期券アプリケーションは移動体端末11-1のメモリ12の他のアプリケーションの中で代金決済を行うことのできるアプリケーションを検索する。より具体的には、定期券アプリケーションを実行している制御部31は、定期券アプリケーションの書き込まれている管理エリア40-1の識別番号と共に、他の管理エリア40およびフリーエリア41に書き込まれているアプリケーション  
20 に対する読み取り要求を、メモリコントローラ35に対し送信する。

メモリコントローラ35は、各管理エリア40およびフリーエリア41に対する制御部31からの読み取り要求を受信すると、まず制御部31から読み取り要求と共に送信された管理エリア40-1の識別情報を用いて、管理エリア40-1の信頼情報領域40Rから信頼度を読み出す。この場合、読み出される信頼度  
25 は「3」である。以下、これを「要求元信頼度」と呼ぶ。

続いて、メモリコントローラ35は、読み取り要求の対象となっている管理エリア40-2、管理エリア40-3、・・・、管理エリア40-nのそれぞれに関して、信頼情報領域40Rから信頼度を読み出す。また、フリーエリア40-1、フリーエリア40-1、・・・、フリーエリア40-mに関しては、信頼度は与え

られていないため、信頼度は「0」として扱われる。このようにして得られる信頼度を、以下、「要求先信頼度」と呼ぶ。

続いて、メモリコントローラ35は、要求元信頼度と各要求先信頼度とを比較し、要求元信頼度が要求先信頼度より高いか等しい場合、すなわち要求先信頼度が「3」以下である場合に限り、読み取り要求を実行し、それ以外の場合に関し

5      ては、制御部31に対し読み取り要求の拒否通知を送信する。

ここで、管理エリア40-2には代金決済の可能な決済アプリケーションがあるが、その要求先信頼度は「5」であるため、メモリコントローラ35は定期券アプリケーションからの決済アプリケーションに対する読み取り要求を拒否する。

10      その結果、定期券アプリケーションは決済アプリケーションの存在を認識できない。従って、定期券アプリケーションはメモリ12内に代金決済を行うことのできるアプリケーションを見つけることができず、移動体端末11-1は画面D45を表示する。画面D45において、ユーザは別途代金の送金手続を行うよう要求される。ユーザは画面D45の情報をメモ用紙等に取り出した後、ボタン「9」

15      を押下して定期券アプリケーションを終了させる。その結果、ディスプレイ部21には通常画面である画面D46が表示される。

続いて、ユーザは画面D46において、再度アプリボタン23を押下し、アプリケーションメニュー（画面D47）を表示させる。ユーザは画面D47においてボタン「3」を押下し、起動するアプリケーションの選択画面（画面D48）

20      を表示する。ユーザは画面D48においてボタン「2」を押下し、決済アプリケーションを選択する。移動体端末11-1は決済アプリケーションを起動し、決済アプリケーションは「xx銀行」のホームページを開く（画面D49）。

画面D49において、ユーザは暗証番号を入力し、処理の選択画面である画面D50を表示させる。画面D50において、ユーザはボタン「3」を押下して、

25      「3. 送金」を選択し、画面D51を表示させる。画面D51において、ユーザは先に取り出した「abc鉄道」への送金情報を入力し、ボタン「9」を押下して送金情報を「xx銀行」のホームページに対し送信する。「xx銀行」は、この送金情報をホームページ経由で移動体端末11-1から受信し、指定された送金処理を「abc鉄道」の口座に対して行った後、移動体端末11-1のディスプ

レイ部 21 に画面 D 5 2 を表示させる。一方、「a b c 鉄道」は「x x 銀行」からの送金を確認し、移動体端末 11-1 による定期乗車券購入の処理を完了し、移動体端末 11-1 に関する購入履歴情報を更新する。

画面 D 5 2 において、ボタン「9」が押下されると、移動体端末 11-1 は通常の画面である画面 D 5 3 を表示する。続いて、ユーザは画面 D 5 3 において、再度アプリボタン 23 を押下し、アプリケーションメニュー（画面 D 5 4）を表示させる。ユーザは画面 D 5 4 においてボタン「3」を押下し、起動するアプリケーションの選択画面（画面 D 5 5）を表示する。ユーザは画面 D 5 5 においてボタン「1」を押下し、定期券アプリケーションを起動する（画面 D 5 6）。

画面 D 5 6 において、ユーザがボタン「4」を押下して「4. 購入履歴閲覧」を選択すると、移動体端末 11-1 は画面 D 5 7 を表示する。画面 D 5 7 において、ユーザがボタン「1」を押下すると、移動体端末 11-1 は、先に購入した定期乗車券の購入履歴明細を表示する（画面 D 5 8）。ユーザは画面 D 5 8 において、先に購入した定期乗車券に対する送金が「a b c 鉄道」により確認され、定期乗車券の購入処理が無事完了したことを確認する。その後、ユーザがボタン「9」を押下すると、移動体端末 11-1 はディスプレイ部 21 に通常の画面である画面 D 5 9 を表示させる。

#### [1. 3. 2] アプリケーション間の関係が許可される場合

以下に説明する例は、信頼度が高いアプリケーションから信頼度が低いアプリケーションもしくは信頼度が同じアプリケーションの機能の呼び出しおよびデータの利用を行うことができることを示す例である。なお、以下の説明には図 3 2、図 3 3、および図 3 4 を用いる。

まず、移動体端末 11-1 の管理エリア 40-1 におけるアプリケーション領域 40 A に、通信販売機能を持つアプリケーション（以下、「通信販売アプリケーション」と呼ぶ）が書き込まれており、アクティベーション処理がなされ利用可能となっている。通信販売アプリケーションを用いると、移動体端末 11-1 のユーザは「サイバー商店 z z」のホームページを開き、そのホームページにおいて商品を購入することができる。この通信販売アプリケーションの信頼度は「4」である。

一方、管理エリア40-2におけるアプリケーション領域40Aには、先の例と同様に、決済アプリケーションが書き込まれており、アクティベーション処理がなされ利用可能となっている。以下、この決済アプリケーションを「決済アプリケーション1」と呼ぶ。決済アプリケーション1の信頼度は「4」である。

- 5      また、管理エリア40-3におけるアプリケーション領域40Aには、クレジットカードによる代金決済機能を持つアプリケーション(以下、「クレジットアプリケーション」と呼ぶ)が書き込まれており、アクティベーション処理がなされ利用可能となっている。クレジットアプリケーションを用いると、移動体端末11-1のユーザは「cc信販」のホームページを開き、そのホームページにおいてクレジットカードによる代金決済の手続きを行うことができる。このクレジットアプリケーションの信頼度は「4」である。

- 15      また、管理エリア40-4におけるアプリケーション領域40Aには、決済アプリケーション1と同様の機能を持つが、「xx銀行」ではなく、「kk銀行」のホームページを開き、送金等の処理を行うことができるアプリケーションが書き込まれており、アクティベーション処理がなされ利用可能となっている。以下、この決済アプリケーションを「決済アプリケーション2」と呼ぶ。決済アプリケーション2の信頼度は「5」である。

- 20      移動体端末11-1のユーザは、アプリボタン23を押下し、アプリケーションメニュー(画面D71)をディスプレイ部21に表示させる。続いて、ユーザは画面D71においてボタン「3」を押下し、起動するアプリケーションの選択画面(画面D72)を表示する。ユーザは画面D72においてボタン「1」を押下し、通信販売アプリケーションを選択する。移動体端末11-1は通信販売アプリケーションを起動し、通信販売アプリケーションは「サイバー商店zz」のホームページを開く(画面D73)。

- 25      画面D73において、ユーザがボタン「2」を押下して牛肉の購入を選択すると、通信販売アプリケーションは、続いて購入申込のされた商品の配送先の入力画面を表示する(画面D74)。画面D74において、ユーザが購入する商品の配送先を入力し、ボタン「9」を押下すると、通信販売アプリケーションは移動体端末11-1のメモリ12の他のアプリケーションの中で代金決済を行うことの

できるアプリケーションを検索する。なお、以下の説明のため、ユーザは商品の配送先として、「東京都新宿区1-1-1」を入力したものとする。代金決済を行うことのできるアプリケーションの検索処理の具体的な流れは、定期券アプリケーションの例において説明したものと同様である。

- 5 代金決済を行うことのできるアプリケーションの検索処理において、通信販売アプリケーションによるメモリ12の他のアプリケーションの読み取り要求が行われる際、要求元である通信販売アプリケーションの信頼度は「4」である。一方、この読み取り要求の要求先の一つである決済アプリケーション1の信頼度は「4」であるため、メモリコントローラ35は通信販売アプリケーションからの
- 10 決済アプリケーション1に対する読み取り要求を承諾し、決済アプリケーション1の機能情報を通信販売アプリケーションを実行している制御部31に送信する。同様に、クレジットアプリケーションの信頼度も「4」であるため、メモリコントローラ35はクレジットアプリケーションの機能情報を制御部31に送信する。それに対し、決済アプリケーション2の信頼度は「5」であり、要求元の通信販
- 15 売アプリケーションの信頼度「4」よりも高いため、メモリコントローラ35は制御部31の決済アプリケーション2に対する読み取り要求を拒否し、通信販売アプリケーションには決済アプリケーション2の機能情報が送信されない。その結果、通信販売アプリケーションは、代金決済を行うことができるアプリケーションとして、決済アプリケーション1およびクレジットアプリケーションの2つ
- 20 が利用可能である、と判断し、画面D75を表示する。

- 画面D75において、ユーザが代金決済の方法として決済アプリケーション1を利用することを選び、ボタン「1」を押下すると、通信販売アプリケーションはメモリコントローラ35に対して、決済アプリケーション1の読み取り要求を送信する。また、通信販売アプリケーションは決済アプリケーション1に対し、
- 25 決済アプリケーション1を読み出す目的およびその目的を実行するために必要な情報を渡す。より具体的には、通信販売アプリケーションを実行している制御部31は、メモリコントローラ35に対し、決済アプリケーション1が管理している管理エリア40-2のデータ領域40D-2に、読み出しの目的が「サイバー商店xx」における牛肉1kgの購入に対する5,000円の送金であり、送金

先が「nn銀行」の口座番号が「4 1 2 5 6 3 7 8」である「普通口座」であり、購入商品の配送先が「東京都新宿区1-1-1」である、という情報の書き込み要求を送信する。

- メモリコントローラ35はアプリケーション読み出しおよびデータ書き込みの要求元信頼度と要求先信頼度の比較を行い、アプリケーションの読み出しとデータの書き込みを承諾する。その結果、制御部31は決済アプリケーション1を起動する。

- 続いて、決済アプリケーション1は画面D76を表示し、移動体端末11-1のユーザに本人確認のための暗証番号の入力を求める。画面D76において、移動体端末11-1のユーザが正しい暗証番号を入力すると、決済アプリケーション1は画面D77を表示する。この際、送金に必要な情報は、決済アプリケーション1により管理エリア40-2のデータ領域40D-2より読み出され、既に画面D77に入力されている。従って、ユーザがそれらの情報を入力する必要はない。

- 画面D77において、ユーザが送金情報を確認し、ボタン「9」を押下すると、決済アプリケーション1は「xx銀行」のホームページに対して送金依頼を送信する。その際、決済アプリケーション1は購入商品情報および購入商品の配送先情報も「xx銀行」のホームページに対し送信する。

- 「xx銀行」は、ホームページを介して移動体端末11-1から送金依頼、購入商品情報、および購入商品の配送先情報を受信すると、「サイバー商店zz」に対して指定された送金を行うとともに、「サイバー商店zz」に対して、購入商品情報および購入商品の配送先情報も送信する。「サイバー商店zz」は「xx銀行」からの送金を確認するとともに、その送金により牛肉1kgの購入がなされ、その牛肉1kgの配送先が「東京都新宿区1-1-1」である、という情報を受け取る。その結果、「サイバー商店zz」は購入された商品の配送処理を行うとともに、移動体端末11-1に対して、商品の配送日および注文番号とともに、入金確認通知を送信する。

移動体端末11-1の制御部31において実行されている決済アプリケーション1は、「サイバー商店zz」より入金確認通知を受信すると、メモリコントローラ



ラ 3 5 に対し、決済アプリケーション 1 の呼び出し元である通信販売アプリケーションの読み出しと、通信販売アプリケーションが管理しているデータ領域 4 0 D-1 への、商品の配送日および注文番号に関するデータの書き込みの要求を行う。この場合においても、メモリコントローラ 3 5 は要求元信頼度と要求先信頼度の比較を行い、これらの要求を承諾する。その結果、制御部 3 1 は処理途中で待機していた通信販売アプリケーションを再度起動し、通信販売アプリケーションはデータ領域 4 0 D-1 に書き込まれた商品の配送日および注文番号に関するデータを読み出し、画面 D 7 8 を表示する。画面 D 7 8 において、ユーザが「サイバー商店 z z」からの送信確認の内容を確認し、ボタン「9」を押下すると、移動体端末 1 1-1 は通常の画面である画面 D 7 9 を表示し、処理を終了する。

このように、信頼度の高いアプリケーションは金銭情報や個人情報のような価値の高い情報を直接、他のアプリケーションから受け取ったり、価値の高い情報を扱う他のアプリケーションの機能呼び出ししたりすることができる。また、信頼度が「5」であるアプリケーションであれば、制御用メモリ 3 2 に格納されている制御用プログラムを呼び出ししたり、それらのプログラムが管理しているデータを利用することもできる。従って、ユーザの操作は簡便化される。しかしながら、既に説明したように、アプリケーションが高い信頼度を得るには管理サーバ 1 6 の管理事業者による審査が必要であり、また信頼度の与えられたアプリケーションに関しては、管理サーバ 1 6 の管理事業者により、必要に応じてアプリケーションの改竄がないことが確認されているため、ユーザは安心して価値の高い情報を扱うアプリケーションを利用することができる。

## 〔2〕第 2 実施形態

第 2 実施形態は、上述した第 1 実施形態と比較し、以下に説明するように第 1 実施形態における信頼度の代わりに信頼関係情報を用いる点が異なっている。その他の点に関しては全て第 1 実施形態と同様である。従って、以下の説明においては第 2 実施形態が第 1 実施形態と異なる点のみを説明する。また、以下の説明においては、各構成要素を特定するために、第 1 実施形態において用いた名称および符号をそのまま用いる。

### 〔2. 1〕権限情報の構成および機能

第2実施形態において、コンテンツサーバ20により管理サーバ16の管理事業者に対しアプリケーションの内容審査の依頼がなされた場合、管理サーバ16の管理事業者は新たに内容審査を行ったアプリケーションと、既に内容審査が行われているアプリケーションのそれぞれとの間に、アプリケーションの読み取り、データの読み取り、データの書き込み、およびデータの削除についての権限を設定する。

以下、識別番号が「AP-3568」であるアプリケーションに関し、新たに内容審査が行われた場合を例とし、具体例を説明する。また、例えば識別番号が「AP-3568」であるアプリケーションを呼ぶ際には、アプリケーション「AP-3568」と呼ぶ。図35はアプリケーション「AP-3568」に関して与えられた権限を示すデータ例である。なお、以下の説明では図35に示す形式のデータを「権限情報」と呼ぶ。

図35の第1列は、アプリケーション「AP-3568」が読み取りを許可されているアプリケーションのリストである。例えば、アプリケーション「AP-3568」を実行している制御部31が、アプリケーション「AP-3712」の機能を利用したい場合、制御部31はメモリコントローラ35に対し、アプリケーション「AP-3712」の読み取り要求を送信する。アプリケーション「AP-3712」はアプリケーション「AP-3568」に対応した権限情報の第1列に含まれている。従って、メモリコントローラ35はアプリケーション「AP-3712」の読み取り要求を受信すると、その読み取り要求を承諾する。そして、メモリコントローラ35はこの読み取り要求を承諾すると、管理エリア40のアプリケーション領域40Aからアプリケーション「AP-3712」を読み出し、読み出したアプリケーションを制御部31に対し送信する。

また、図35の第2列は、アプリケーション「AP-3568」がデータの読み取りを許可されているアプリケーションのリストである。例えば、アプリケーション「AP-3568」を実行している制御部31が、アプリケーション「AP-8125」の管理するデータの読み取りを行いたい場合、制御部31はメモリコントローラ35に対し、アプリケーション「AP-8125」の管理するデータの読み取り要求を送信する。ここで、アプリケーション「AP-8125」

はアプリケーション「AP-3568」の権限情報の第2列に含まれている。従って、メモリコントローラ35はアプリケーション「AP-8125」の管理するデータの読み取り要求を受信すると、その読み取り要求を承諾する。そして、メモリコントローラ35は読み取り要求を承諾すると、アプリケーション「AP-8125」が格納されている管理エリア40のデータ領域40Dから要求されたデータを読み出し、読み出したデータを制御部31に対し送信する。

図35の第3列および第4列は、それぞれ、アプリケーション「AP-3568」が、データの書き込みを許可されているアプリケーションのリスト、およびデータの削除を許可されているアプリケーションのリストである。

一方、図35の第5列は、アプリケーション「AP-3568」を読み取ることが許可されているアプリケーションのリストである。例えば、アプリケーション「AP-4315」を実行している制御部31が、アプリケーション「AP-3568」の機能を利用したい場合、制御部31はメモリコントローラ35に対し、アプリケーション「AP-3568」の読み取り要求を送信する。ここで、アプリケーション「AP-4315」はアプリケーション「AP-3568」の権限情報の第5列に含まれている。従って、メモリコントローラ35はアプリケーション「AP-4315」によるアプリケーション「AP-3568」の読み取り要求を受信すると、その読み取り要求を承諾する。そして、メモリコントローラ35は読み取り要求を承諾すると、管理エリア40のアプリケーション領域40Aからアプリケーション「AP-3568」を読み出し、読み出したアプリケーションを制御部31に対し送信する。

同様に、権限情報の第6列、第7列、および第8列は、それぞれ、アプリケーション「AP-3568」が管理するデータを、読み取ることが許可されているアプリケーションのリスト、書き込むことが許可されているアプリケーションの一覧、および削除することが許可されているアプリケーションのリストである。

## 〔2. 2〕信頼関係情報の登録および更新

管理サーバ16のアプリケーション情報格納部52の登録アプリケーション領域52Rには、図36に示すように、第1実施形態における信頼度の項目の代わりに、信頼関係情報の項目が設けられている。管理サーバ16の管理事業者は、

新たにアプリケーション「AP-3568」の内容審査を行うと、図35に示した権限情報を管理サーバ16に入力する。管理サーバ16は、権限情報が入力されると、登録アプリケーション領域52Rにアプリケーション「AP-3568」に対応するデータを新たに作成し、その信頼関係情報に関する項目に、権限情報の第5列から第8列までを格納する。

続いて、管理サーバ16は、権限情報の第1列から第4列のそれぞれに含まれる全てのアプリケーションに関し、登録アプリケーション領域52Rにおいて対応するデータの信頼関係情報に関する項目を更新する。例えば、アプリケーション「AP-3712」はアプリケーション「AP-3568」の権限情報の第1列に含まれているので、管理サーバ16は登録アプリケーション領域52Rにおけるアプリケーション「AP-3712」に対応するデータの信頼関係情報に関する項目の、アプリケーション読み取りの項目に、アプリケーション「AP-3568」を追加する。

次に、管理サーバ16は、ユーザ情報格納部53-1、ユーザ情報格納部53-2、・・・、ユーザ情報格納部53-kの既配信アプリケーション領域53Aのデータを読み出し、上記において信頼関係情報が更新されたアプリケーション、すなわちアプリケーション「AP-3568」の権限情報の第1列から第4列に含まれるアプリケーションの識別番号を含むユーザ情報格納部53を、アプリケーション「AP-3568」の権限情報の各列ごとに抽出する。続いて管理サーバ16は、抽出されたユーザ情報格納部53の信頼関係情報の対応する項目に、アプリケーション「AP-3568」を追加する。その後、管理サーバ16は、アプリケーション「AP-3568」の追加を行ったユーザ情報格納部53に対応する移動体端末11に対し、ユーザ情報格納部53における信頼関係情報の対応する項目にアプリケーション「AP-3568」が追加されたことを通知する。例えば、ユーザ情報格納部53-1のデータ例を示す図7によれば、移動体端末11-1はメモリ12の管理エリア40-2のアプリケーション領域40A-2にアプリケーション「AP-0123」を書き込んでいる。アプリケーション「AP-0123」は図35に示した権限情報の第1列に含まれ、新たに内容審査の行われたアプリケーション「AP-3568」にはアプリケーション「AP-0

1 2 3」に対するアプリケーションの読み取り権限が与えられている。従って、管理サーバ16は移動体端末11-1に対し、ユーザ情報格納部53-1のアプリケーション「AP-0123」の信頼関係情報のアプリケーション読み取りに関する項目に、新たにアプリケーション「AP-3568」が追加されたことを通知する。

各移動体端末11においては、内容審査の行われているアプリケーションをメモリ12にダウンロードする場合、アプリケーションとともに対応する信頼関係情報が添付されてダウンロードされる。移動体端末11のメモリコントローラ35は、ダウンロードしたアプリケーションに添付されている信頼関係情報を、アプリケーションを書き込む管理エリア40の信頼情報領域40Rに書き込む。

従って、例えば移動体端末11-1が、先に示した例のように管理サーバ16より、ユーザ情報格納部53-1のアプリケーション「AP-0123」の信頼関係情報のアプリケーション読み取りに関する項目に、新たにアプリケーション「AP-3568」が追加されたことに関する通知を受信すると、移動体端末11-1のメモリコントローラ35は、アプリケーション「AP-0123」が書き込まれている管理エリア40-2の信頼情報領域40R-2のデータにおける、アプリケーション読み取りの項目に、アプリケーション「AP-3568」を追加する。

以上の処理により、アプリケーション情報格納部52の登録アプリケーション領域52R、および各移動体端末11における管理エリア40の信頼情報領域40Rのデータは常に最新のものに更新される。

### 〔2.3〕信頼関係情報を用いたアプリケーション連係動作の制御

各移動体端末11において、あるアプリケーションが他のアプリケーションの機能を利用したり、他のアプリケーションの管理するデータを利用する場合には、制御部31は処理要求と共に、処理の要求先のアプリケーションの書き込まれているメモリエリアの識別番号（以下、「要求先エリア番号」と呼ぶ）、および処理の要求元のアプリケーションの識別番号をメモリコントローラ35に送信する。

要求先エリア番号により指定されたメモリエリアが管理エリア40である場合、メモリコントローラ35は制御部31より処理要求を受信すると、その管理エリ

- ア 40 の信頼情報領域 40 R から信頼関係情報を読み出す。続いて、メモリコントローラ 35 は要求元のアプリケーションの識別番号が、読み出した信頼関係情報において、処理要求の内容に対応する項目に含まれているかどうかを確認する。
- 例えば、アプリケーション「AP-2568」を実行している制御部 31 が、メモリコントローラ 35 に対し、アプリケーション領域 40 A-2 に書き込まれている「AP-0123」に対するアプリケーションの読み取り要求を送信した場合、メモリコントローラ 35 は信頼情報領域 40 R-2 から信頼関係情報を読み出し、そのアプリケーションの読み取りが許可されているアプリケーションのリストにアプリケーション「AP-2568」が含まれているかどうかを確認する。
- 10 要求元のアプリケーションがこのリストに含まれている場合、メモリコントローラ 35 は制御部 31 の処理要求を承諾し、要求に従った処理を行う。一方、要求元のアプリケーションが、読み取りが許可されているアプリケーションのリストに含まれていない場合、メモリコントローラ 35 は制御部 31 の処理要求を拒否する。
- 15 このようなメモリコントローラ 35 による信頼関係情報を利用した制御により、アプリケーション間の連係動作において、きめ細かい管理が可能となる。

### 〔3〕第 3 実施形態

- 第 3 実施形態は、上述した第 1 実施形態と比較し、以下に説明するようにアプリケーションの配信の流れが異なっている。その他の点に関しては全て第 1 実施形態と同様である。従って、以下の説明においては第 3 実施形態が第 1 実施形態と異なる点のみを説明する。また、以下の説明においては、各構成要素を特定するために、第 1 実施形態において用いた名称および符号をそのまま用いる。
- 20

#### 〔3. 1〕アプリケーション配信システムの構成

- まず、第 1 実施形態と同様に、コンテンツサーバ 20 の管理事業者が希望する場合、アプリケーションの内容は管理サーバ 16 の管理事業者により審査され、信頼度が与えられる。その際、第 3 実施形態においては、管理サーバ 16 の管理事業者は、アプリケーションに対しハッシュ関数を用いて、メッセージダイジェストを作成する。ハッシュ関数は元となるデータから、不可逆的なデータを作成するので、このメッセージダイジェストからは、それに対応するアプリケーション
- 25

- ンを復元することはできない。また、わずかでも内容の異なるアプリケーションからは、同じメッセージダイジェストが作成されることは極めて稀であり、実用上、アプリケーションの内容がわずかでも変更されれば、同じハッシュ関数を用いてそのアプリケーションから作成されるメッセージダイジェストは、変更前の
- 5 アプリケーションに対応するメッセージダイジェストとは一致しない。なお、メッセージダイジェストはそれに対応するアプリケーションのサイズと比較して小さく、格納容量が少なくて済む上、送受信が容易である。管理サーバ16の管理事業者は、作成したメッセージダイジェストを信頼度とともにアプリケーション情報格納部52に格納する。図37は、第3実施形態においてアプリケーション
- 10 情報格納部52に格納されるデータ例を示す図である。

なお、第3実施形態においては、説明の簡易化のため、内容審査の行われたアプリケーションに関し、管理サーバ16において移動体端末11に対し、アプリケーションの一覧を公開することは行わないものとする。従って、図37において、公開に関する項目は設けられていない。

- 15 第3実施形態においては、第1実施形態と異なり、アプリケーション本体はアプリケーション情報格納部52に格納されることはなく、全て配信元である各コンテンツサーバ20に格納される。従って、図37において、保管場所に関する項目にアプリケーション本体が格納されているアプリケーションはなく、全てのアプリケーションについて、保管場所を示すURLが格納されている。

- 20 第3実施形態においては、第1実施形態と異なり、アプリケーション本体は全て、直接、配信元である各コンテンツサーバ20から各移動体端末11に配信される。従って、管理サーバ16のアプリケーション情報格納部52において、一時保管アプリケーション領域52Tは不要であるため、設けられていない。また、管理サーバ16のユーザ情報格納部53においても、第1実施形態において、一時保管アプリケーション領域52Tに格納されるアプリケーションの保管場所を
- 25 特定するために設けられていた保管番号の項目は不要であるため、設けられていない。図38は第3実施形態におけるアプリケーションの情報管理システムの構成を示す図であり、図39は第3実施形態におけるユーザ情報格納部53に格納されるデータ例を示す図である。

また、第3実施形態においては、移動体端末11-1のメモリコントローラ35は、管理サーバ16からメッセージダイジェストを受信するとそれを一時的に格納する。また、移動体端末11-1のメモリコントローラ35は、通信部34を介して「1」以上の信頼度の与えられたアプリケーションを受信すると、受信したアプリケーションのメッセージダイジェストを作成し、その新たに作成されたメッセージダイジェストを、管理サーバ16から受信されるメッセージダイジェストと照合する。

### [3. 2] アプリケーションの配信

移動体端末11のユーザが、「1」以上の信頼度を与えられているアプリケーションの購入およびダウンロードを行う処理の例として、移動体端末11-1のユーザが、コンテンツサーバ20-1が配信元であるアプリケーションを購入し、ダウンロードする場合の処理を図40、図41、および図42を用いて説明する。また、以下の処理の流れに伴い、移動体端末11-1のディスプレイ部21に表示される表示は、第1実施形態におけるアプリケーションのダウンロード処理において用いた図21と同様であるので、それを用いる。

移動体端末11-1のユーザは、例えば移動体端末11-1を用いてコンテンツサーバ20-1内のホームページを開き、そのホームページにおいて目的のアプリケーションの購入申請を行う（ステップS601）。その際、移動体端末11-1のユーザは購入するアプリケーションの利用料金の支払手続も行うものとする。

コンテンツサーバ20-1は移動体端末11-1の購入申請の内容が所定の条件を満たしていることを確認した後、管理サーバ16に対しアプリケーションの購入承諾通知を送信する（ステップS602）。この購入承諾通知にはアプリケーションの購入を行った移動体端末11-1の識別番号と、購入されたアプリケーションの識別番号が含まれている。また、コンテンツサーバ20-1は購入承諾通知を送信する際、購入承諾を行った移動体端末11-1の識別番号を記録する。

管理サーバ16は、コンテンツサーバ20-1から購入承諾通知を受信すると、受信した購入承諾通知に含まれている移動体端末の識別番号からアプリケーションを購入した移動体端末を特定する。続いて管理サーバ16は、移動体端末11



ー 1 に対応するユーザ情報格納部 5 3 - 1 における配信可能アプリケーション領域 5 3 B に、購入承諾通知に含まれているアプリケーションの識別番号を登録する（ステップ S 6 0 3）。

5 続いて、管理サーバ 1 6 は、移動体端末 1 1 - 1 に対し、アプリケーションの購入処理の完了通知を送信する（ステップ S 6 0 4）。移動体端末 1 1 - 1 は、アプリケーションの購入処理の完了通知を受信すると、ディスプレイ部 2 1 の上部に「α」を表示する。この「α」の表示は、移動体端末 1 1 - 1 のユーザに対し、新たにダウンロードが可能となったアプリケーションがあることを知らせるための表示である。

10 ここで、コンテンツサーバ 2 0 - 1 により管理サーバ 1 6 に対して、新たに購入が行われたアプリケーションの料金徴収の代行依頼がされている場合には、管理サーバ 1 6 はアプリケーションの識別番号、移動体端末 1 1 - 1 の識別番号、購入日時等の情報を課金管理サーバに送信する（ステップ S 6 0 5）。

15 移動体端末 1 1 - 1 のユーザは、移動体端末 1 1 - 1 のアプリボタン 2 3 を押下して、画面 D 2 1 のアプリケーションメニューを表示させる。画面 D 2 1 において、移動体端末 1 1 - 1 のユーザは、操作部 2 2 のボタン「2」を押下して「2. アプリケーションのダウンロード」を選択する。ボタン「2」が押下されると、移動体端末 1 1 - 1 は管理サーバ 1 6 に対し、ダウンロードの可能なアプリケーション情報一覧の送信要求を行う（ステップ S 6 0 6）。

20 管理サーバ 1 6 はアプリケーション情報一覧の送信要求を受信すると、ユーザ情報格納部 5 3 - 1 の配信可能アプリケーション領域 5 3 B に登録されているアプリケーションの名称を、アプリケーションの識別番号と共にアプリケーション情報一覧として移動体端末 1 1 - 1 に送信する（ステップ S 6 0 7）。

25 移動体端末 1 1 - 1 はアプリケーション情報一覧を受信すると、画面 D 2 2 を表示させる。これに対し、移動体端末 1 1 - 1 のユーザは対応する番号のボタンを押下することにより、ダウンロードするアプリケーションの指定を行う。例えばユーザが画面 D 2 2 においてボタン「1」を押下すると、「スケジュール管理 Ver. 2」という名称のアプリケーションが選択される。移動体端末 1 1 - 1 のユーザによるボタン操作によりアプリケーションが指定されると、移動体端末

11-1は管理サーバ16に対し、指定されたアプリケーションの識別番号を送信する（ステップS608）。

管理サーバ16は指定されたアプリケーションの識別番号を受信すると、管理サーバ16は既配信アプリケーション領域53Aのデータを読み出し、移動体端末11-1のメモリ12の管理エリア40に、指定されたアプリケーションを書き込むために必要な空き容量があるかどうかを確認する（ステップS609）。

ステップS609において、移動体端末11-1のメモリ12に指定されたアプリケーションを書き込むための空き容量が十分でない場合、管理サーバ16は移動体端末11-1に対し、メモリ12上から削除すべきアプリケーションの指定要求を送信する（ステップS610）。移動体端末11-1はこの指定要求を受信すると、画面D23をディスプレイ部21に表示させる。移動体端末11-1のユーザがこの画面に対しボタン「9」を押下して実行の指示を行うと、移動体端末11-1はさらに画面D24をディスプレイ部21に表示させる。画面D24には管理エリア40に書き込まれているアプリケーションの名称が表示される。

この画面において、移動体端末11-1のユーザは対応するボタンを押下することにより、メモリ12から削除するアプリケーションを指定する。移動体端末11-1は指定されたアプリケーションの識別番号を管理サーバ16に送信する（ステップS611）。なお、ステップS611の処理の後、移動体端末11-1はディスプレイ部21に画面D25を表示させる。

一方、ステップS609において、指定されたアプリケーションを書き込むための空き容量が移動体端末11-1のメモリ12に十分ある場合、ステップS610およびステップS611の処理は行われず、管理サーバ16は次のステップS612の処理に進む。また、移動体端末11-1はディスプレイ部21に画面D25を表示させる。

続いて、管理サーバ16は、移動体端末11-1により指定されたアプリケーションの識別番号を用いて、アプリケーション情報格納部52から指定されたアプリケーションに対応する内容証明書、信頼度、およびアプリケーションの保管場所に関する情報を読み出し、それらを移動体端末11-1に送信する（ステップS612）。

移動体端末 11-1 は、管理サーバ 16 よりアプリケーションの内容証明書、信頼度、およびアプリケーションの保管場所に関する情報を受信すると、受信したアプリケーションの保管場所に関する情報を用いて、コンテンツサーバ 20-1 に対し、アプリケーションの送信要求を送信する（ステップ S 613）。このアプリケーションの送信要求には、移動体端末 11-1 の識別番号およびアプリケーションの識別番号が含まれている。

コンテンツサーバ 20-1 は、アプリケーションの送信要求を受信すると、受信した送信要求に含まれる移動体端末の識別番号が、ステップ S 602 においてアプリケーションの購入承諾を行った移動体端末の識別番号と一致するかどうかを確認する。これらの識別番号が一致する場合、コンテンツサーバ 20-1 は、認証サーバ 17 に対し移動体端末 11-1 の公開鍵「PK-MT-1」の送信を要求する（ステップ S 614）。認証サーバ 17 は「PK-MT-1」の送信要求を受信すると、コンテンツサーバ 20-1 に対し「PK-MT-1」を送信する（ステップ S 615）。

コンテンツサーバ 20-1 は「PK-MT-1」を受信すると、送信要求のされたアプリケーションを「PK-MT-1」を用いて暗号化する（ステップ S 616）。この暗号化処理により、アプリケーションがコンテンツサーバ 20-1 から移動体端末 11-1 に配信される際、第 3 者がこれを傍受しても内容を解読することができず、アプリケーションが第 3 者により不正に使用されることが防がれる。

コンテンツサーバ 20-1 は暗号化されたアプリケーションを移動体端末 11-1 に対し送信する（ステップ S 617）。

移動体端末 11-1 は暗号化されたアプリケーションを受信すると、そのアプリケーションを移動体端末 11-1 の秘密鍵「SK-MT-1」を用いて復号化する（ステップ S 618）。

続いて、移動体端末 11-1 は、ステップ S 608 の処理により平文となったアプリケーションのメッセージダイジェストを作成し、作成したメッセージダイジェストと、ステップ S 612 において管理サーバ 16 より受信した内容証明書との照合を行う（ステップ S 619）。ここで、管理サーバ 16 においてアプリケ

ーションの内容審査直後に作成されたメッセージダイジェストである内容証明書と、新たに作成されたメッセージダイジェストが一致すると、移動体端末11-1がコンテンツサーバ20-1より受信したアプリケーションが、内容審査後に変更されていないことが証明される。もしこれらのメッセージダイジェストが一致しない場合、アプリケーションの内容が変更されているので、移動体端末11-1は、そのアプリケーションのメモリ12への書き込みを行わず、管理サーバ16に対し、正しいアプリケーションの受信に失敗したことを通知する。

ステップS619において、2つのメッセージダイジェストが一致した場合、移動体端末11-1は、アプリケーションをメモリ12の管理エリア40のアプリケーション領域40Aのいずれかに書き込む（ステップS620）。ここで、ステップS609においてメモリ空き容量が残っていなかった場合は、ステップS611において削除の指定を行ったアプリケーションが書き込まれている管理エリア40に、新たに受信されたアプリケーションが書き込まれる。また、ステップS609においてメモリ空き容量が残っていた場合は、空いている管理エリア40のいずれかに、新たに受信されたアプリケーションが書き込まれる。

移動体端末11-1は、アプリケーションの書き込みを完了すると、管理サーバ16に対し、アプリケーションの書き込み完了通知を送信する（ステップS621）。移動体端末11-1はステップS621の処理を終えると、ディスプレイ部21に通常の画面である画面D26を表示させる。

管理サーバ16は、アプリケーションの書き込み完了通知を受信すると、ユーザ情報格納部53のデータの更新を行う（ステップS622）。具体的には、まず移動体端末11のメモリ12より削除されたアプリケーションがある場合、そのアプリケーションの情報を既配信アプリケーション領域53Aから配信可能アプリケーション領域53Bに移動する。次に、新たにメモリ12に書き込まれたアプリケーションの情報を、配信可能アプリケーション領域53Bから既配信アプリケーション領域53Aの対応する場所に移す。

以上が、移動体端末11のユーザが、「1」以上の信頼度を与えられているアプリケーションの購入およびダウンロードを行う処理の流れである。これに対し、移動体端末11のユーザが、信頼度「0」のアプリケーションの購入およびダウ

ンロードを行う場合は、管理サーバ16による移動体端末11-1に対する内容証明書および信頼度の送信は不要である。従って、図40におけるステップS601～ステップS604、ステップS606～ステップS611、ステップS613～ステップS618、ステップS620～ステップS622のみが行われる。

- 5    なお、この場合、ステップS610およびステップS611において、削除候補のアプリケーションの一覧は管理エリア40に書き込まれたアプリケーションではなく、フリーエリア41に書き込まれたアプリケーションの一覧となる。

- 10    以上により、アプリケーションが移動体端末11-1のメモリ12に書き込まれるが、そのアプリケーションはアクティベーション処理がなされていない。従って、移動体端末11-1のユーザは、続いてアクティベーション処理を行うことにより新たに購入したアプリケーションを利用することができるようになる。その場合のアクティベーション処理は、第1実施形態において説明したアクティベーション処理と同様である。また、第3実施形態においても、第1実施形態と同様にディアクティベーション処理、および削除処理を行うことができる。

15    〔4〕実施形態の変形例

〔4.1〕第1変形例

- 20    第1変形例においては、アプリケーション配信システムには複数の管理サーバが含まれている。これらの複数の管理サーバは、例えば互いに同期が取られ、常時データベースのデータが更新されているため、各移動体端末および各コンテンツサーバは管理サーバとの間で処理を行う場合、応答の速い管理サーバを自由に選択することができる。第1変形例においては、管理サーバにより分散処理が可能となるので、アプリケーション配信システム全体の処理速度の向上と、管理サーバの障害発生に対する信頼性の向上が実現される。

〔4.2〕第2変形例

- 25    第2変形例においては、移動体端末においてアプリケーションを書き込む場所として、移動体端末に内蔵されたメモリに加え、各種のICカードメモリ、UIM (User Identification Module)、および移動体端末に装着可能な外部記憶装置がユーザにより自由に選択できる。従って、第2変形例においては、移動体端末間でアプリケーションの記録媒体を交換することに

より、アプリケーションを共有したり、移動させたりすることが容易である。

[4. 3] 第3変形例

- 第3変形例においては、移動体端末は他の情報端末と有線もしくは無線で移動体通信網を介さずに接続可能な入出力インタフェースを持っている。従って、移動体端末はその入出力インタフェースを介して他の情報端末からアプリケーションを取得することができる。

[4. 4] 第4変形例

- 第4変形例においては、管理サーバはアプリケーション情報格納部において、内容が同一のアプリケーションであっても、配信元が異なるものについては異なるアプリケーション識別番号を与え、必要に応じて異なる信頼性に関する情報を与えている。従って、例えば、信頼度の高いコンテンツプロバイダから送信されるアプリケーションには高い信頼度が与えられ、信頼度の低いコンテンツプロバイダから配信されるアプリケーションには低い信頼度が与えられており、同じアプリケーションであっても加える制限を変更可能である。

15 [4. 5] 第5変形例

第5変形例においては、移動体端末のメモリにおいて、1つのアプリケーションが複数のメモリエリアを利用することができる。従って、移動体端末において、プログラムサイズの大きいアプリケーションの実行が可能である。

[4. 6] 第6変形例

- 第6変形例においては、内容審査の行われているアプリケーションの書き込まれる管理エリアと、内容審査の行われていないアプリケーションの書き込まれるフリーエリアの領域を自由に変更することができる。メモリーコントローラは各メモリエリアに書き込まれているアプリケーションに信頼性に関する情報が与えられているかどうかを管理しているため、管理エリアのアプリケーションとフリーエリアのアプリケーションが混同されることはない。従って、例えば管理エリアの空き容量が不足した場合、フリーエリアの空き容量を管理エリアに切り換えることにより、メモリエリアの効率的利用ができる。

25 [4. 7] 第7変形例

第7変形例においては、アプリケーションの内容審査および信頼性に関する情

報の付与は管理サーバの管理事業者とは異なる第3者機関が行う。第3者機関により付与されるアプリケーションの信頼性に関する情報は、随時管理サーバに送信され、管理サーバおよび移動体端末により利用される。

また、この第3者機関が管理する内容認証サーバは、コンテンツサーバから管理サーバにアプリケーションが送信される際、アプリケーションの内容に対しコンテンツサーバによる改竄等が行われていないことを証明するための証明書を、管理サーバに対し発行する。

より具体的には、第3者機関はアプリケーションの内容審査を行った後、そのアプリケーションに対しハッシュ関数を用いてメッセージダイジェストを作成する。管理サーバはコンテンツサーバからアプリケーションを受信すると、内容認証サーバに対し、そのアプリケーションに対応するメッセージダイジェストの送信を要求する。内容認証サーバは要求に応じてメッセージダイジェストを管理サーバに送信する。管理サーバはメッセージダイジェストを受信すると、アプリケーションに対し第3者機関が用いたものと同じハッシュ関数を用いてメッセージダイジェストを作成し、内容認証サーバから受信したメッセージダイジェストと、新たに作成したメッセージダイジェストを照合する。この照合処理により、管理サーバは受信したアプリケーションの内容が正しいことを確認できる。

第7変形例においては、第3者機関が内容の保証を行うので、管理サーバは平文のアプリケーションを取得する必要はない。従って、コンテンツサーバは、例えば移動体端末の公開鍵で暗号化したアプリケーションを管理サーバ経由で移動体端末に配信することができる。また、管理サーバはアプリケーションの内容そのものに変更のないことを確認できるので、そのアプリケーションの送信元を確認する必要がない。従って、コンテンツサーバは、コンテンツサーバの秘密鍵でアプリケーションを暗号化することなく、管理サーバに送信することができる。

#### 25 [4. 8] 第8変形例

第8変形例においては、あるアプリケーションが、他のアプリケーションもしくは制御用プログラムの機能を利用したり、他のアプリケーションもしくは制御用プログラムの管理するデータを利用したりする場合、アプリケーションもしくは制御用プログラムにおける機能単位、およびデータの種別単位に利用の許可も

しくは拒否を判定するための信頼関係情報が設定されている。

従って、第8実施例においては、例えば、移動体端末において、アプリケーションAがアプリケーションBの機能1は利用できるが、アプリケーションBの機能2は利用できない、といったきめ細かい制御を行うことができる。

#### 5   〔5〕実施形態の効果

以上の説明のように、本発明の方法、システム、および装置によれば、移動体端末の有するメモリに格納された複数のアプリケーション間の連係動作が可能となる。その一方で、メモリコントローラがアプリケーション間のデータの受け渡しや機能の相互利用を、各アプリケーションに与えられる信頼性に関する情報を  
10   用いて厳しく管理するため、個人情報や金銭情報等の価値の高い情報が漏洩したり破壊される危険性が低減される。その結果、移動体端末におけるアプリケーションの利用において、ユーザの使い勝手の向上と情報セキュリティの確保を両立することができる。



## 請求の範囲

1. 移動体端末が、移動体端末において動作するプログラムを取得し、メモリに格納するプログラム取得過程と、

- 5 前記移動体端末が、前記プログラムによる他のプログラムの起動および他のプログラムとの間のデータの授受の少なくとも一方の制御に用いられる連係制御情報を取得し、メモリに格納する連係制御情報取得過程と、

- 前記移動体端末が、前記メモリに格納された1のプログラムの実行中に、他のプログラムの実行要求が発生したとき、実行中のプログラムに対応する前記連係  
10 制御情報に基づいて、他のプログラムの起動および他のプログラムとの間のデータの授受の態様を決定するプログラム制御過程と  
を備えることを特徴とするプログラム管理方法。

2. 請求項1に記載のプログラム管理方法であって、

- 15 前記移動体端末は、前記連係制御情報取得過程において、前記連係制御情報を、通信網を介して管理サーバから取得すること  
を特徴とするプログラム管理方法。

3. 請求項1に記載のプログラム管理方法であって、

- 20 前記移動体端末は、前記プログラム取得過程において、前記プログラムを、通信網を介して配信サーバから取得すること  
を特徴とするプログラム管理方法。

4. 請求項1に記載のプログラム管理方法であって、

- 25 通信網を介して前記移動体端末と通信可能な内容証明サーバが、前記プログラムおよび前記連係制御情報のいずれかもしくは両方の内容が正当であることを示す証明情報を作成する証明情報作成過程と、

前記移動体端末が、前記通信網を介して、前記内容証明サーバから前記証明情報を取得する証明情報取得過程と、

前記移動体端末は、前記証明情報に基づいて、前記移動体端末における前記プログラムの動作を許可もしくは禁止すること  
を特徴とするプログラム管理方法。

5 5. 請求項4に記載のプログラム管理方法であって、

前記証明情報は、暗号鍵による前記プログラムおよび前記連係制御情報のいずれかもしくは両方の暗号化により作成され、

前記移動体端末は、暗号化された前記プログラムおよび前記連係制御情報のいずれかもしくは両方について復号化可能な場合に、前記プログラムの動作を許可  
10 すること

を特徴とするプログラム管理方法。

6. 請求項5に記載のプログラム管理方法であって、

前記暗号鍵は、公開鍵方式における秘密鍵であること

15 を特徴とするプログラム管理方法。

7. 請求項4に記載のプログラム管理方法であって、

前記証明情報は、前記プログラムおよび前記連係制御情報のいずれかもしくは両方を要約したメッセージダイジェストであり、

20 前記移動体端末は、前記証明情報と、前記プログラムおよび前記連係制御情報のいずれかもしくは両方について前記移動体端末が作成するメッセージダイジェストとの照合結果に基づき、前記プログラムの動作を許可すること  
を特徴とするプログラム管理方法。

25 8. 請求項2に記載のプログラム管理方法であって、さらに、

前記管理サーバが、前記移動体端末における前記プログラムの格納状態に関する格納データを作成する格納データ作成過程と、

前記管理サーバが、前記格納情報に基づいて、前記移動体端末における前記プログラムの管理に関する管理データを作成する管理データ作成過程と、

前記移動体端末が、前記管理データを、前記管理サーバから取得する管理データ取得過程と

を備え、

- 5 前記移動体端末は、前記管理データに基づいて、前記移動体端末における前記プログラムの管理を行うこと  
を特徴とするプログラム管理方法。

9. 請求項 8 に記載のプログラム管理方法であって、

- 10 前記移動体端末は、前記管理データに基づいて、前記移動体端末における前記プログラムの動作を許可もしくは禁止すること  
を特徴とするプログラム管理方法。

10. 請求項 9 に記載のプログラム管理方法であって、

- 15 前記移動体端末は、前記移動体端末における前記プログラムの動作を許可する場合、文字、画像、音、振動の一部もしくは全てにより、前記プログラムの動作が許可されたことを通知すること  
を特徴とするプログラム管理方法。

11. 請求項 8 に記載のプログラム管理方法であって、

- 20 前記移動体端末は、前記管理データに基づいて、前記移動体端末における前記プログラムを削除すること  
を特徴とするプログラム管理方法。

12. 請求項 8 に記載のプログラム管理方法であって、

- 25 前記通信網は、さらに、前記プログラムの利用料金を管理する課金サーバを含み、

前記課金サーバが、前記管理データの一部もしくは全てを課金データとして取得する課金データ取得過程を備え、

前記課金サーバは、前記課金データに基づいて、前記プログラムの利用料金の

管理を行うこと

を特徴とするプログラム管理方法。

1 3. 請求項 2 に記載のプログラム管理方法であって、さらに、

- 5 前記管理サーバが、プログラムの配信準備要求を取得する配信準備要求取得過程と、

前記管理サーバが、前記配信準備要求に基づいて、前記移動体端末に対する前記プログラムに関する配信準備を行う配信準備過程とを備え、

- 10 前記プログラム取得過程において、前記移動体端末は、前記配信準備過程において配信準備のなされた前記プログラムを取得すること  
を特徴とするプログラム管理方法。

1 4. 請求項 1 3 に記載のプログラム管理方法であって、

- 15 前記配信準備過程において、前記管理サーバは、前記プログラム本体もしくは前記プログラムの所在情報のいずれかもしくは両方を準備すること  
を特徴とするプログラム管理方法。

1 5. 請求項 1 3 に記載のプログラム管理方法であって、さらに、

- 20 前記管理サーバが、前記配信準備過程が完了した時点で、配信準備完了通知を、前記移動体端末に送信する配信準備完了通知送信過程と、

前記移動体端末が、前記配信準備完了通知を、前記管理サーバより受信する配信準備完了通知受信過程とを備え、

- 25 前記移動体端末は、前記配信準備完了通知を受信した時点で、文字、画像、音、振動の一部もしくは全てにより、前記プログラムの配信が可能となったことを通知すること  
を特徴とするプログラム管理方法。

16. 請求項13に記載のプログラム管理方法であって、

前記通信網は、さらに、前記プログラムの利用料金を管理する課金サーバを含み、

5 前記管理サーバが、前記配信準備要求に基づいて、前記移動体端末に対する前記プログラムの配信準備が行われたことを示す配信準備データを作成する配信準備データ作成過程と、

前記課金サーバが、前記配信準備データの一部もしくは全てを課金データとして取得する課金データ取得過程と

を備え、

10 前記課金サーバは、前記課金データに基づいて、前記プログラムの利用料金の管理を行うこと

を特徴とするプログラム管理方法。

17. 配信サーバ、管理サーバ、および移動体端末を含む通信網において、

15 配信サーバは、

プログラムを格納するプログラム格納部と、

前記プログラムを、前記移動体端末に配信するプログラム配信部とを備え、

前記管理サーバは、

20 前記プログラムに対応する連係制御情報を格納する連係制御情報格納部と、前記連係制御情報を、前記移動体端末に送信する連係制御情報送信部とを備え、

前記移動体端末は、

前記プログラムを、前記配信サーバより受信するプログラム受信部と、

25 前記連係制御情報を、前記管理サーバより受信する連係制御情報受信部と、前記プログラムを記憶するプログラム記憶部と、

前記連係制御情報を記憶する連係制御情報記憶部と、

前記プログラムの1つの実行中に、他のプログラムの実行要求が発生したとき、実行中のプログラムに対応する前記連係制御情報に基づいて、他のプログラムの

起動および他のプログラムとの間のデータの授受の態様を決定するプログラム制御部と

を備えることを特徴とするプログラム管理システム。

5 18. 移動体端末を含む通信網において、

前記移動体端末において、あるプログラムの実行中に、他のプログラムの実行要求が発生したとき、他のプログラムの起動および他のプログラムとの間のデータの授受の態様を決定するために用いられる連係制御情報を格納する連係制御情報格納部と、

10 前記連係制御情報を、前記移動体端末に送信する連係制御情報送信部と  
を備えることを特徴とする管理サーバ。

19. 請求項18に記載の管理サーバであって、さらに、

前記プログラムおよび前記連係制御情報のいずれかもしくは両方の内容が正当  
15 であることを示す証明情報を作成する証明情報作成部と、  
前記証明情報を、前記移動体端末に送信する証明情報送信部と  
を備えることを特徴とする管理サーバ。

20. 請求項19に記載の管理サーバであって、

20 前記証明情報作成部は、前記プログラムおよび前記連係制御情報のいずれかもしくは両方を暗号化する暗号化部を備える  
ことを特徴とする管理サーバ。

21. 請求項20に記載の管理サーバであって、

25 前記暗号化部は、公開鍵方式における秘密鍵を格納する秘密鍵格納部を備える  
ことを特徴とする管理サーバ。

22. 請求項19に記載の管理サーバであって、

前記証明情報作成部は、前記プログラムおよび前記連係制御情報のいずれかも

しくは両方を要約したメッセージダイジェストを作成するメッセージダイジェスト作成部を備える

ことを特徴とする管理サーバ。

5 23. 請求項18に記載の管理サーバであって、さらに、

前記移動体端末における前記プログラムの格納状態に関する格納データを作成する格納データ作成部と、

前記格納データに基づいて、前記移動体端末における前記プログラムの管理に関する管理データを作成する管理データ作成部と、

10 前記管理データを、前記移動体端末に送信する管理データ送信部とを備えることを特徴とする管理サーバ。

24. 請求項23に記載の管理サーバであって、さらに、

15 前記管理データの一部もしくは全てを課金データとして、前記通信網に含まれる課金サーバに対し送信する課金データ送信部を備えることを特徴とする管理サーバ。

25. 請求項18に記載の管理サーバであって、さらに、

20 前記プログラム配信部に対し前記プログラムの配信準備を要求する配信準備要求を受信する配信準備要求受信部と、

前記配信準備要求に基づいて、前記移動体端末に対する前記プログラムの配信準備を行う配信準備部と

を備えることを特徴とする管理サーバ。

25 26. 請求項25に記載の管理サーバであって、

前記配信準備部は、前記プログラム本体もしくは前記プログラムの所在情報のいずれかもしくは両方を記録する準備情報記録部を備える

ことを特徴とする管理サーバ。

27. 請求項25に記載の管理サーバであって、さらに、  
前記配信準備が完了した時点で、配信準備完了通知を、前記移動体端末に送信  
する配信準備完了通知送信部を備える  
ことを特徴とする管理サーバ。

5

28. 請求項25に記載の管理サーバであって、さらに、  
前記配信準備要求に基づいて、前記移動体端末に対する前記プログラムの配信  
準備が行われたことを示す配信準備データを作成する配信準備データ作成部と、  
前記配信準備データの一部もしくは全てを課金データとして、前記通信網に含  
10 まれる課金サーバに対し送信する課金データ送信部と  
を備えることを特徴とする管理サーバ。

29. プログラムを記憶するプログラム記憶部と、  
関係制御情報を記憶する関係制御情報記憶部と

15 前記プログラムの実行中に、他のプログラムの実行要求が発生したとき、前記  
関係制御情報に基づいて、他のプログラムの起動および他のプログラムとの間の  
データの授受の態様を決定するプログラム制御部と  
を備えることを特徴とする移動体端末。

20 30. 配信サーバと管理サーバを含む通信網において、  
プログラムを、前記配信サーバより受信するプログラム受信部と、  
前記プログラムを記憶するプログラム記憶部と、  
関係制御情報を、前記管理サーバより受信する関係制御情報受信部と、  
前記関係制御情報を記憶する関係制御情報記憶部と、

25 前記プログラムの実行中に、他のプログラムの実行要求が発生したとき、前記  
関係制御情報に基づいて、他のプログラムの起動および他のプログラムとの間の  
データの授受の態様を決定するプログラム制御部と  
を備えることを特徴とする移動体端末。



3 1. 請求項 3 0 に記載の移動体端末であって、さらに、

前記プログラムおよび前記連係制御情報のいずれかもしくは両方の内容が正当であることを示す証明情報を、前記管理サーバより受信する証明情報受信部と、  
前記証明情報に基づき、前記プログラムの動作を許可もしくは禁止する動作許

5 可部と

を備えることを特徴とする移動体端末。

3 2. 請求項 3 1 に記載の移動体端末であって、

前記動作許可部は、前記プログラムおよび前記連係制御情報のいずれかもしくは  
10 は両方が暗号化されている場合、暗号化されている前記プログラムおよび前記連  
係制御情報のいずれかもしくは両方を復号化する復号化部を備える  
ことを特徴とする移動体端末。

3 3. 請求項 3 2 に記載の移動体端末であって、さらに

15 前記復号化部は、公開鍵方式における前記管理サーバの公開鍵を格納する公開  
鍵格納部を備える

ことを特徴とする移動体端末。

3 4. 請求項 3 1 に記載の移動体端末であって、

20 前記動作許可部は、前記プログラムおよび前記連係制御情報のいずれかもしくは  
は両方を要約したメッセージダイジェストを作成するメッセージダイジェスト作  
成部を備える

ことを特徴とする移動体端末。

25 3 5. 請求項 3 0 に記載の移動体端末であって、さらに、

前記プログラムの管理に関する管理データを、前記管理サーバから受信する管  
理データ受信部と、

前記管理データに基づいて、前記プログラムの管理を行う管理部と  
を備えることを特徴とする移動体端末。

36. 請求項35に記載の移動体端末であって、さらに、

- 前記管理部が前記プログラムの動作を許可する場合、文字、画像、音、振動の一部もしくは全てにより、前記プログラムの動作が許可されたことを通知する通知部を備えることを特徴とする移動体端末。

37. 請求項30に記載の移動体端末であって、さらに、

- 前記プログラムの配信準備を要求する配信準備要求を、前記管理サーバに送信する配信準備要求送信部を備えることを特徴とする移動体端末。

38. 請求項37に記載の移動体端末であって、さらに、

- 前記配信準備要求に対する配信準備が完了したことを通知する配信準備完了通知を、前記管理サーバより受信する配信準備完了通知受信部と、前記配信準備完了通知を受信した時点で、文字、画像、音、振動の一部もしくは全てにより、前記プログラムの配信が可能となったことを通知する通知部とを備えることを特徴とする移動体端末。

39. 通信網に含まれる移動体端末において、あるプログラムの実行中に、他のプログラムの実行要求が発生したとき、他のプログラムの起動および他のプログラムとの間のデータの授受の態様を決定するために用いられる連係制御情報を、前記移動体端末に送信する連係制御情報送信処理を管理サーバのコンピュータに実行させるプログラム。

40. 請求項39に記載のプログラムであって、さらに、

- 前記移動体端末において実行されるプログラムおよび前記連係制御情報のいずれかもしくは両方の内容が正当であることを示す証明情報を作成する証明情報作成処理と、

前記証明情報を送信する証明情報送信処理と  
を管理サーバのコンピュータに実行させるプログラム。

4 1. 連係制御情報を取得する連係制御情報取得処理と、

- 5 あるプログラムの実行中に、他のプログラムの実行要求が発生したとき、前記連係制御情報に基づいて、他のプログラムの起動および他のプログラムとの間のデータの授受の態様を決定するプログラム制御処理と  
を移動体端末のコンピュータに実行させるプログラム。

- 10 4 2. 請求項 4 1 に記載のプログラムであって、さらに、

前記あるプログラム、前記他のプログラムおよび前記連係制御情報のいずれかもしくは全ての内容が正当であることを示す証明情報を取得する証明情報取得処理と、

- 15 前記証明情報に基づき、前記あるプログラム、および前記他のプログラムのいずれかもしくは両方の動作を許可もしくは禁止する動作許可処理と  
を移動体端末のコンピュータに実行させるプログラム。

- 4 3. 通信網に含まれる移動体端末において、あるプログラムの実行中に、他のプログラムの実行要求が発生したとき、他のプログラムの起動および他のプログラムとの間のデータの授受の態様を決定するために用いられる連係制御情報を、  
20 前記移動体端末に送信する連係制御情報送信処理  
を管理サーバのコンピュータに実行させるプログラムを記録した記録媒体。

4 4. 請求項 4 3 に記載のプログラムであって、さらに、

- 25 前記移動体端末において実行されるプログラムおよび前記連係制御情報のいずれかもしくは両方の内容が正当であることを示す証明情報を作成する証明情報作成処理と、

前記証明情報を送信する証明情報送信処理と  
を管理サーバのコンピュータに実行させるプログラムを記録した記録媒体。

45. 関係制御情報を取得する関係制御情報取得処理と、

あるプログラムの実行中に、他のプログラムの実行要求が発生したとき、前記関係制御情報に基づいて、他のプログラムの起動および他のプログラムとの間の

5 データの授受の態様を決定するプログラム制御処理と

を移動体端末のコンピュータに実行させるプログラムを記録した記録媒体。

46. 請求項45に記載のプログラムであって、さらに、

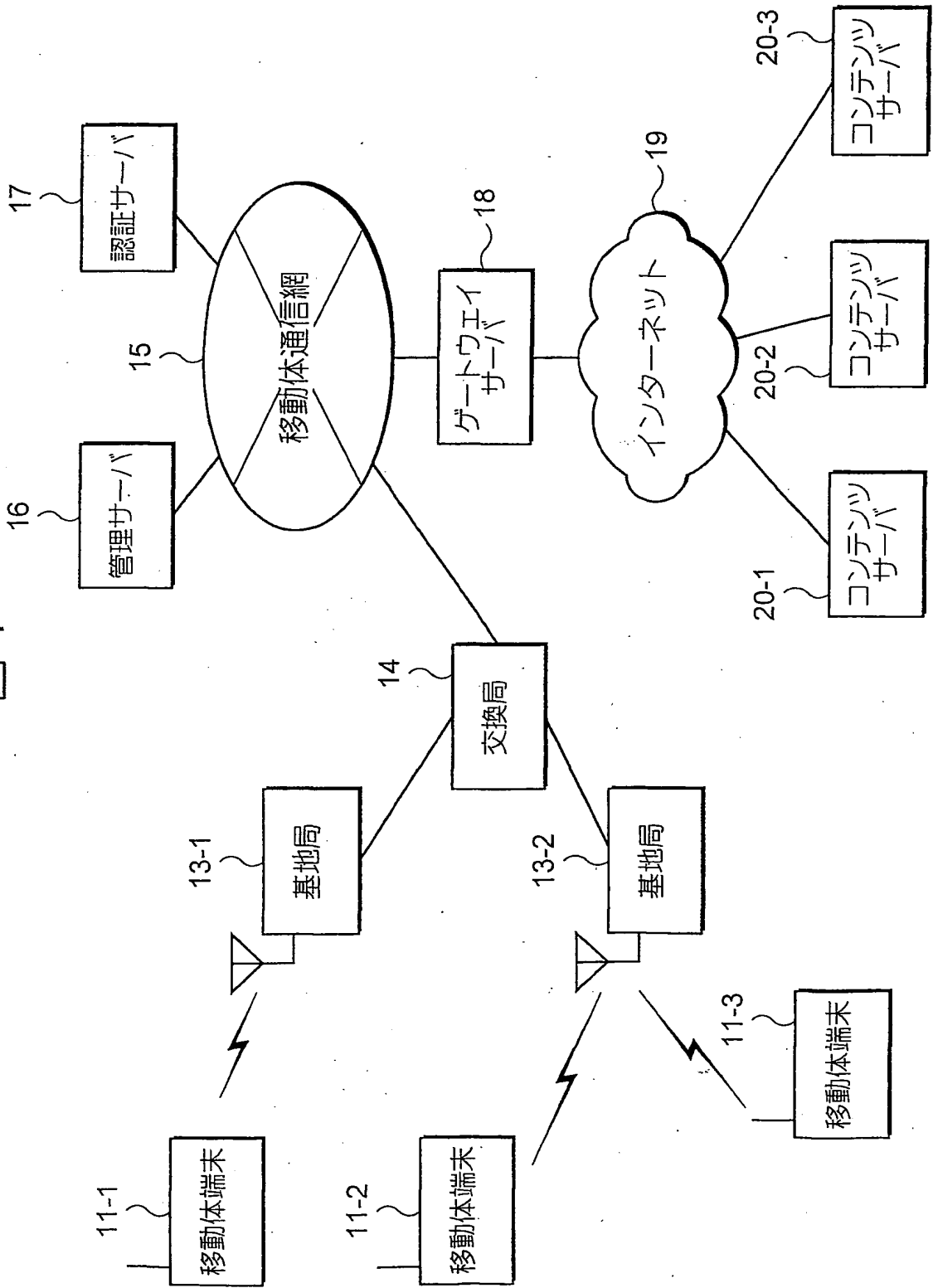
前記あるプログラム、前記他のプログラム、および前記関係制御情報のいずれ  
10 かもしくは全ての内容が正当であることを示す証明情報を取得する証明情報取得  
処理と、

前記証明情報に基づき、前記あるプログラムおよび前記他のプログラムのいずれ  
れかもしくは両方の動作を許可もしくは禁止する動作許可処理と

を移動体端末のコンピュータに実行させるプログラムを記録した記録媒体。

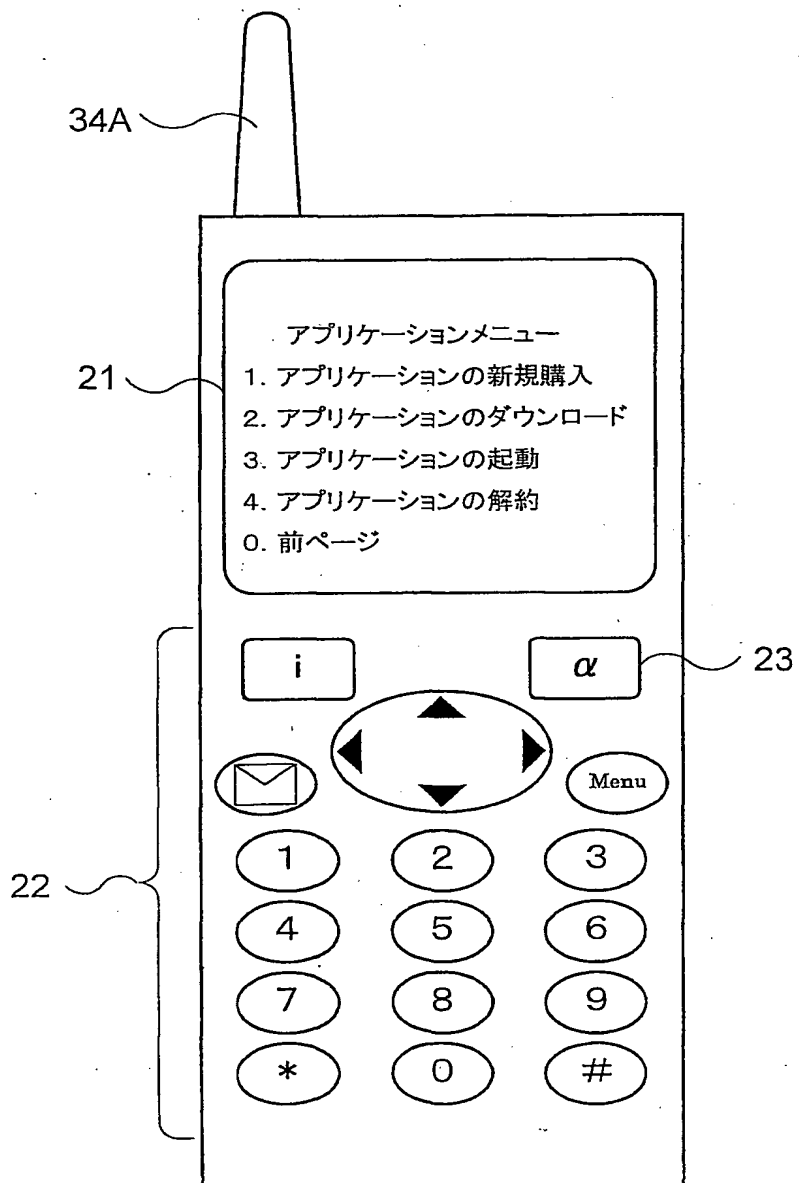
15

図 1



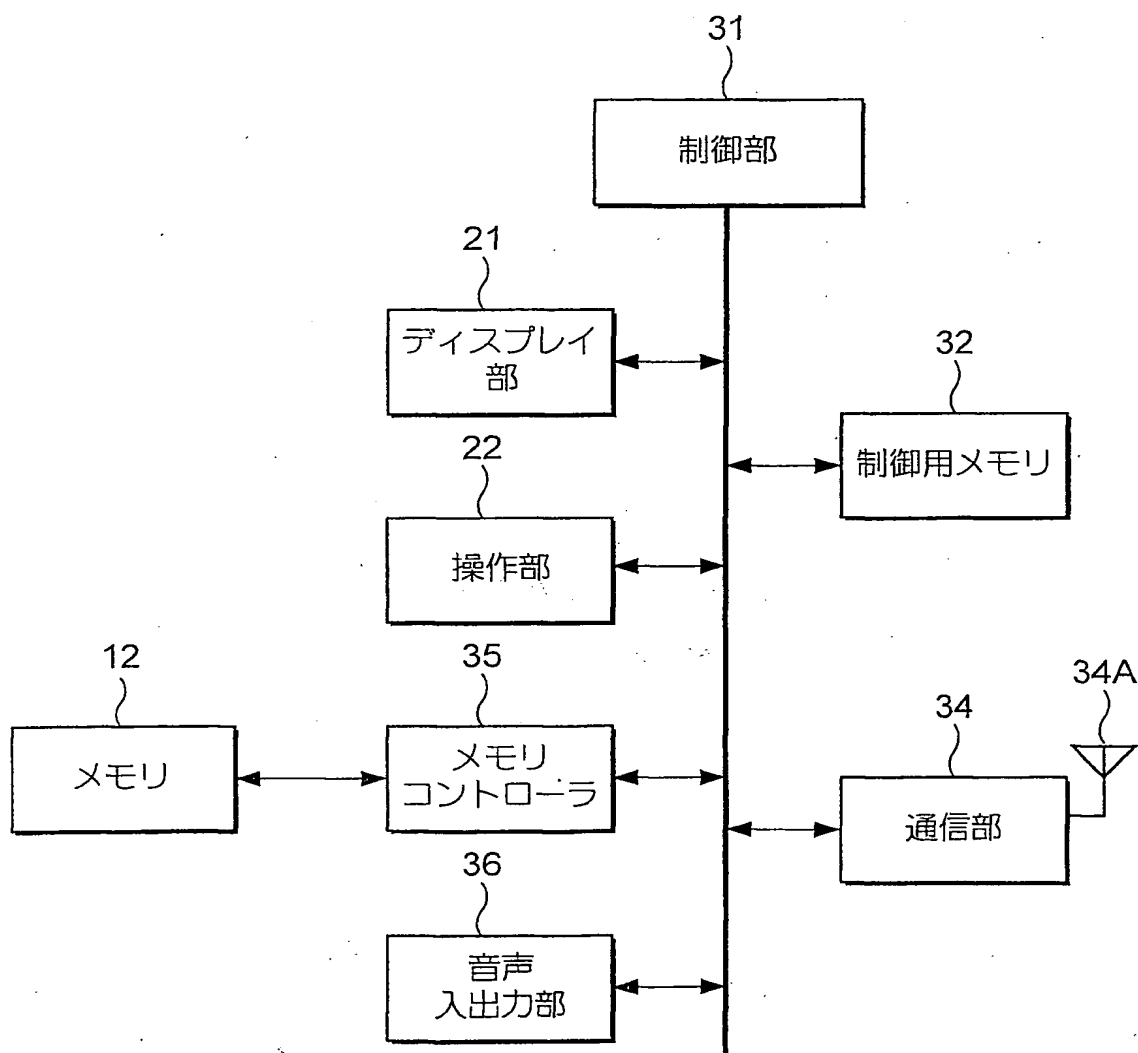
2/41

図 2

11-1

3/41

図 3



4/41

図 4

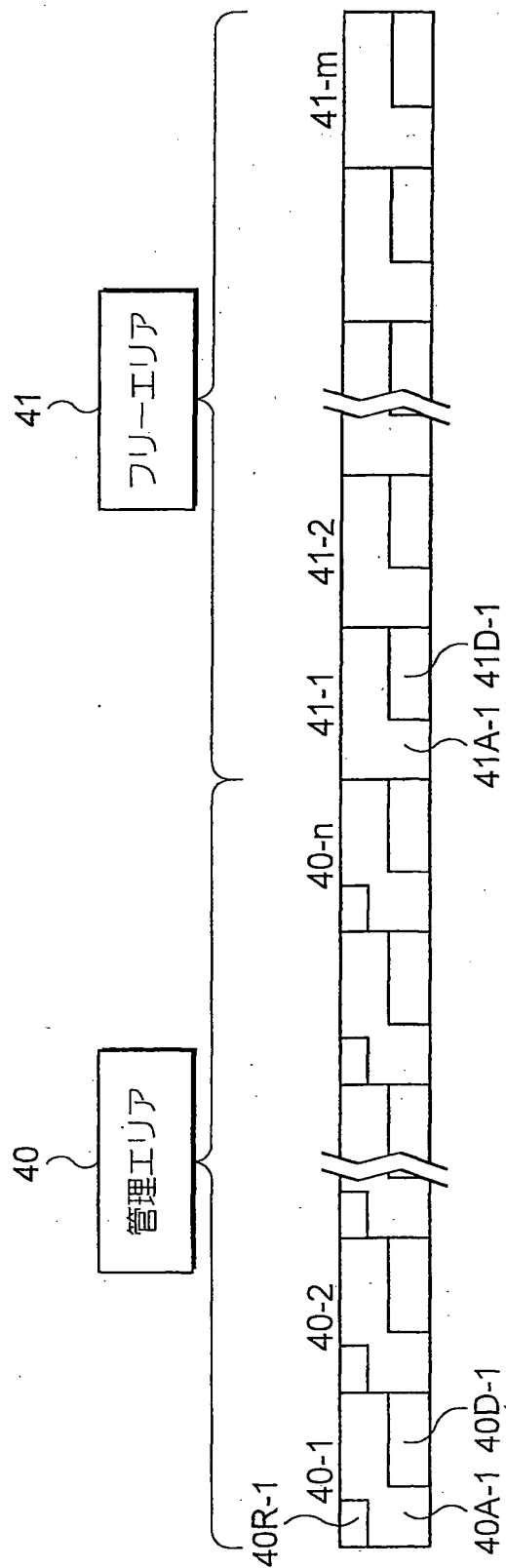
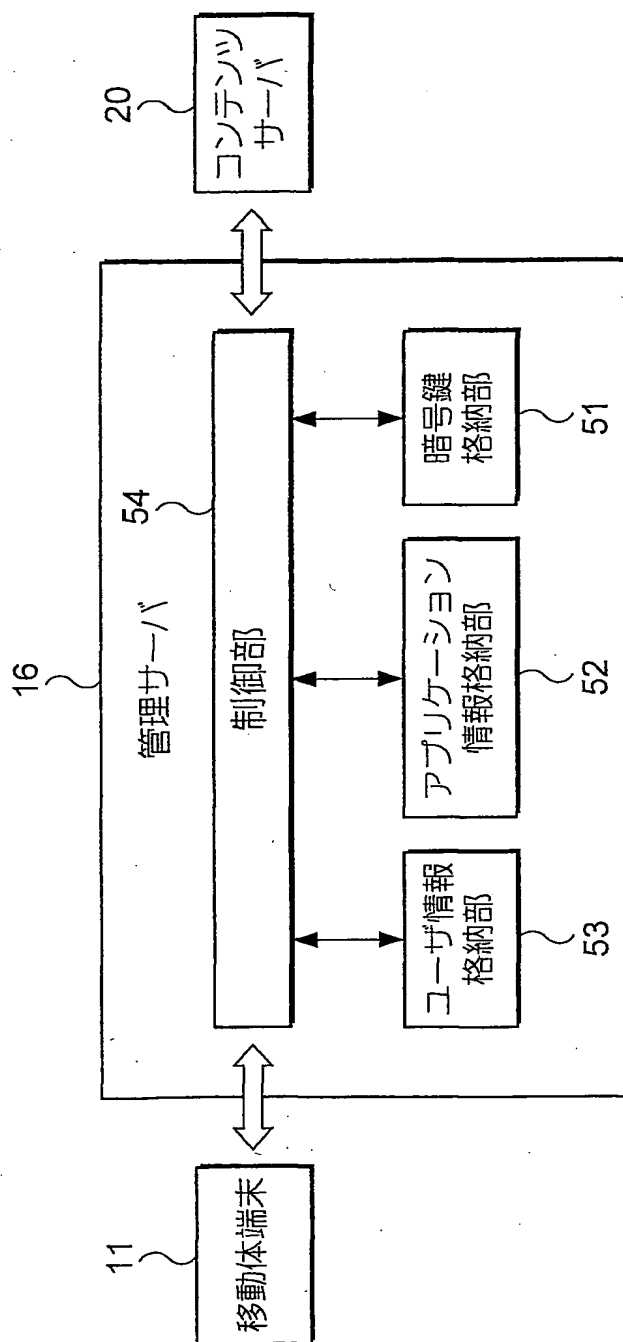


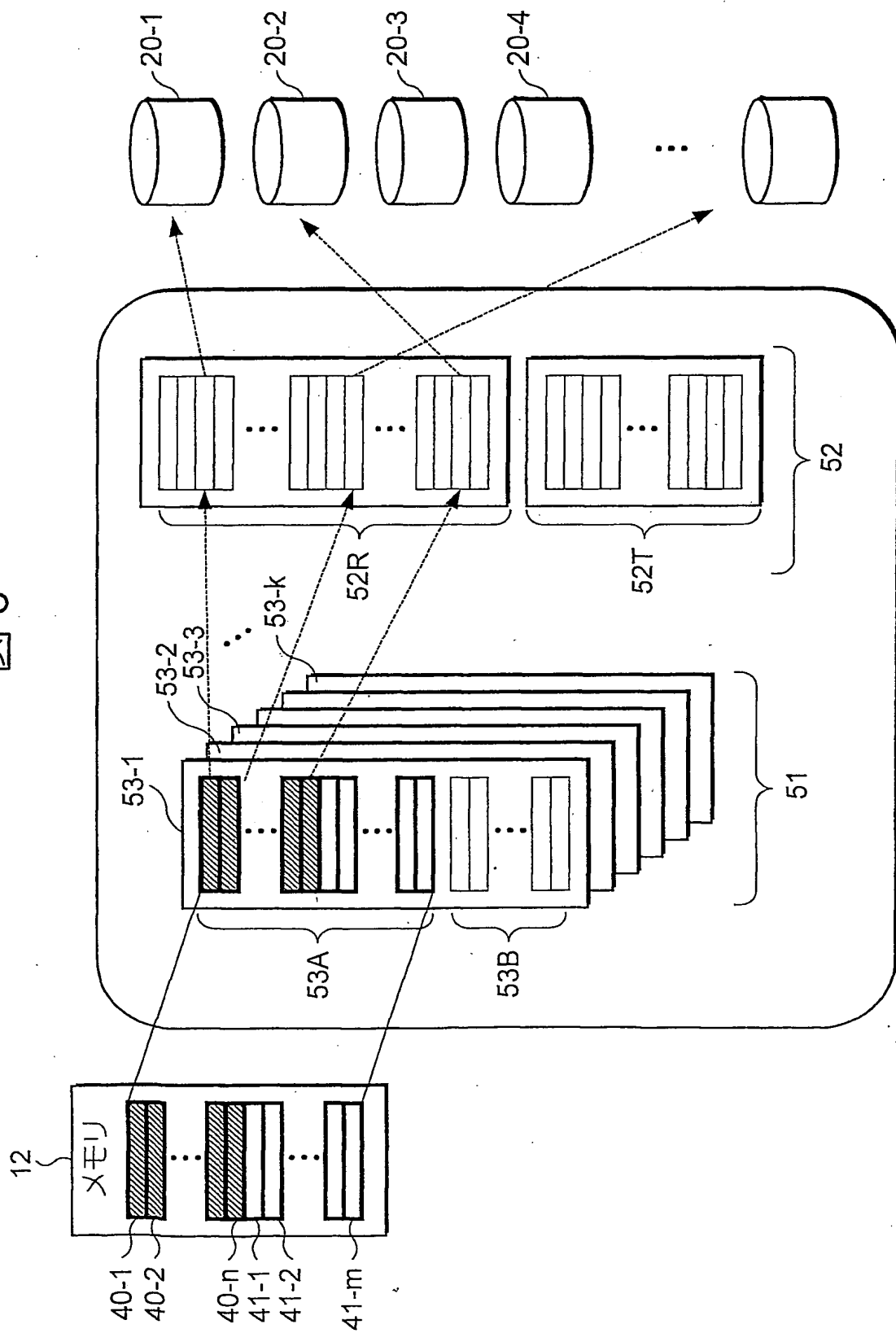


図 5



6/41

図 6



7/41

図 7

	メモリ エリア		アプリケーション 識別番号	アクティベーション	保管番号
既配信アプリケーション領域	管理エリア	1	AP-2568	Yes	—
		2	AP-0123	No	—
		3	AP-1015	Yes	—
		⋮	⋮	⋮	⋮
		n	未使用	—	—
	フリーエリア	1	F-0325	Yes	—
		2	F-7485	Yes	—
		3	未使用	—	—
		⋮	⋮	⋮	⋮
		m	未使用	—	—
配信可能アプリケーション領域			1	AP-4125	—
			2	F-5963	—
			3	AP-3021	削除済み
			4	AP-4513	—
			5	未使用	—
			6	未使用	—
			7	未使用	—
			8	未使用	—
			9	未使用	—
			⋮	⋮	⋮

8/41

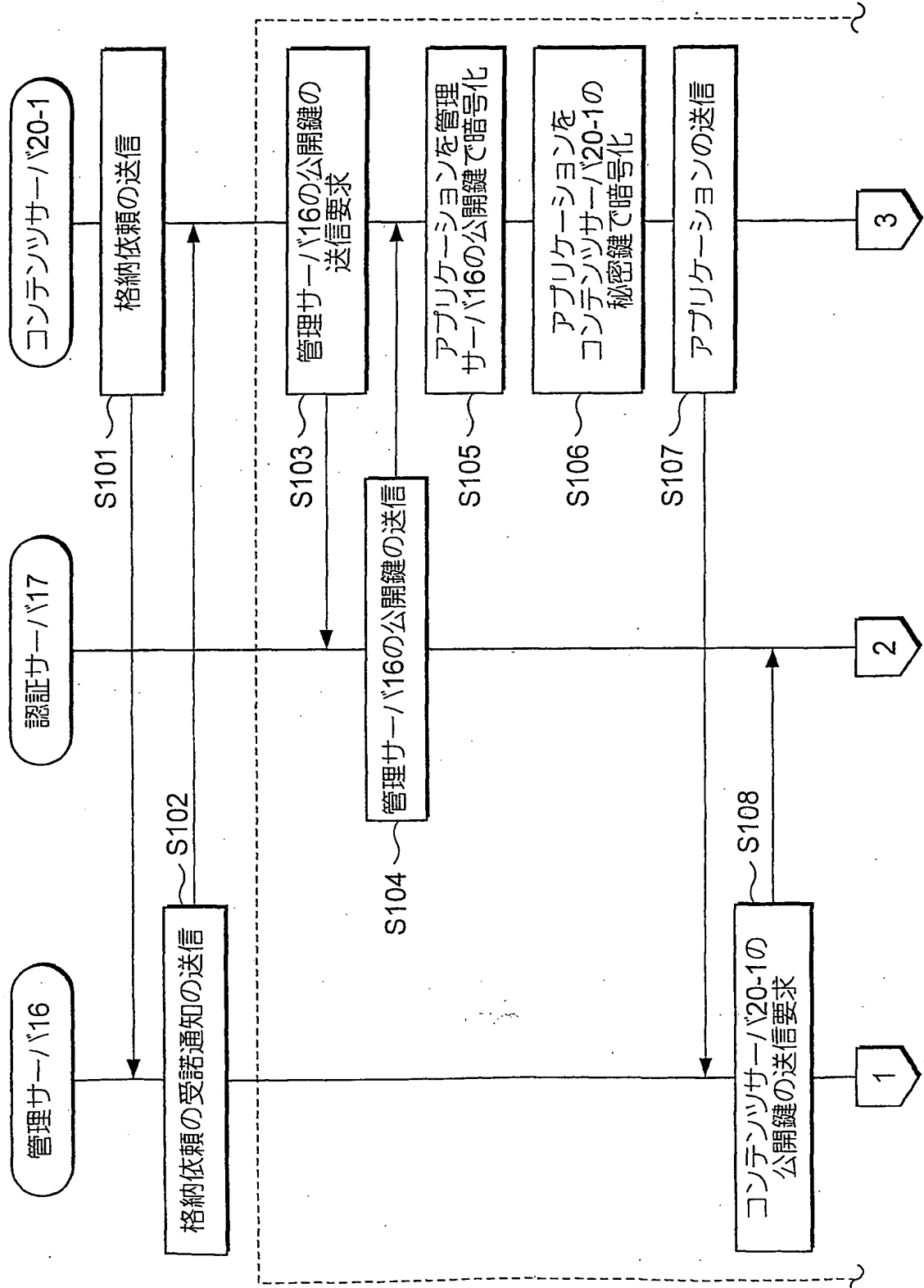
図 8

アプリケーション 識別番号	信頼度	公開	料金徴収	保管場所
AP-2568	3	Yes	Yes	アプリケーション本体を格納
AP-3712	5	Yes	No	ftp://ftp.abc_software.com/application/ap_0306.exe
AP-4513	2	No	Yes	アプリケーション本体を格納
AP-3021	1	No	No	ftp://ftp.software_world.com/software/app_view.exe
F-3251	0	—	—	ftp://ftp.softpocket.com/root/app/miracle.exe
⋮	⋮	⋮	⋮	⋮

図 9

保管番号	
T-1025	アプリケーション本体
T-7851	アプリケーション本体
T-3639	アプリケーション本体
T-7142	アプリケーション本体
T-3256	アプリケーション本体
⋮	⋮

図 10



10/41

図 11

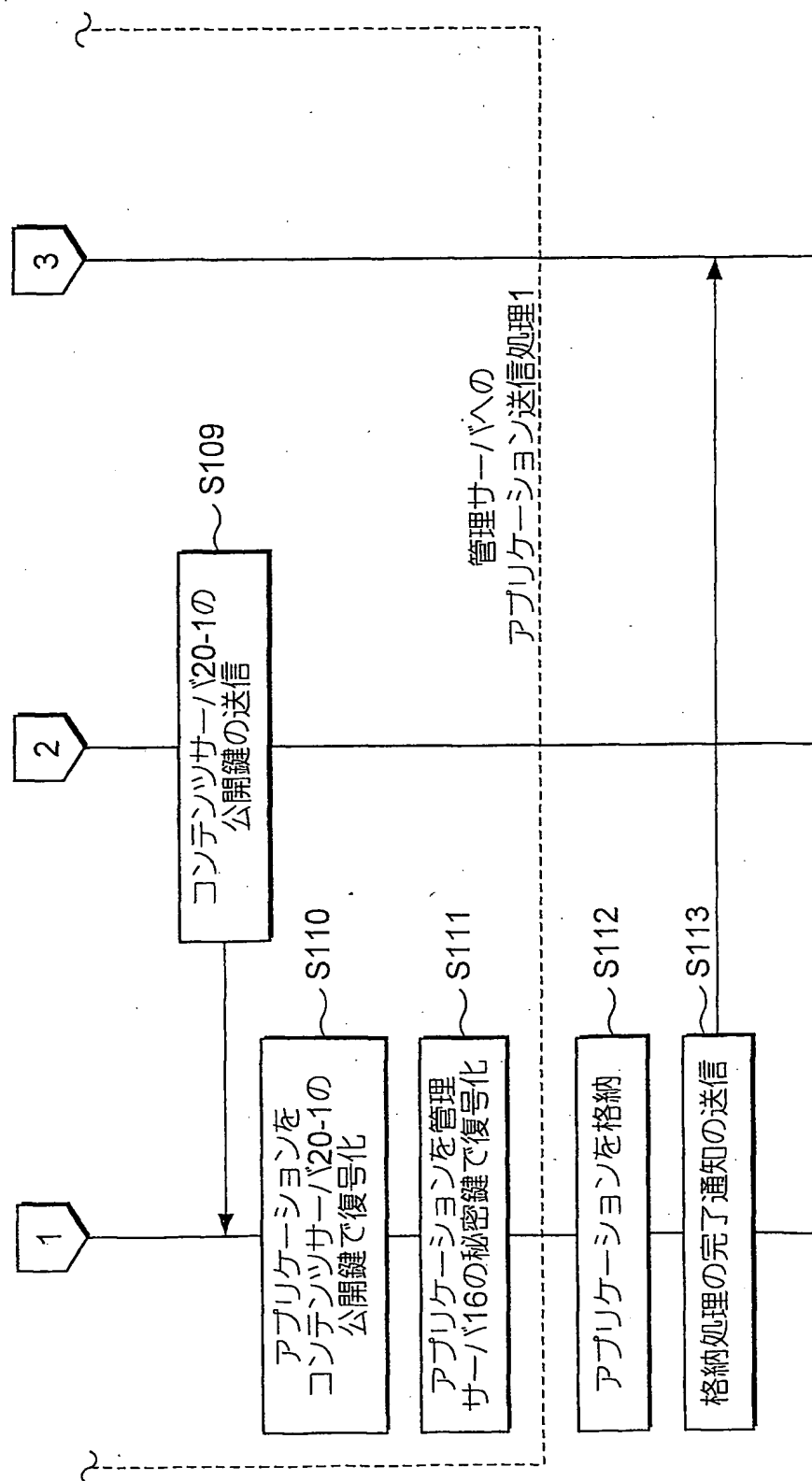


図 12

D11

- アプリケーションメニュー
1. アプリケーションの新規購入
  2. アプリケーションのダウンロード
  3. アプリケーションの起動
  4. アプリケーションの解約
  0. 前ページ

D13

- スケジュール管理 Ver. 2
- 機能:  
簡単にスケジュールが管理できます。  
利用料金: 200円/月
9. 購入
  0. 前ページ

D12

- 購入可能アプリケーション
1. スケジュール管理 Ver. 2
  2. シューティングゲーム Ver. 7
  3. カード決着 Ver. 3
  4. eショッピング Ver. 5
  9. 次ページ
  0. 前ページ

D14

- スケジュール管理 Ver. 2
- の購入手続中です。  
しばらくお待ち下さい。

12/41

図 13

D15

スケジュール管理 Ver. 2  
の購入手続が完了しました。  
なお、利用料金は通信料金と共に請求  
されます。

9. 終了

D17

 $\alpha$ 

電話番号

D16

スケジュール管理 Ver. 2  
の購入手続が完了しました。  
なお、利用料金の支払手続を以下のサ  
イトにて行って下さい。

[http://www.software\\_abc.co](http://www.software_abc.co)  
m/

0. サイトに移動

9. 終了





14/41

図 15

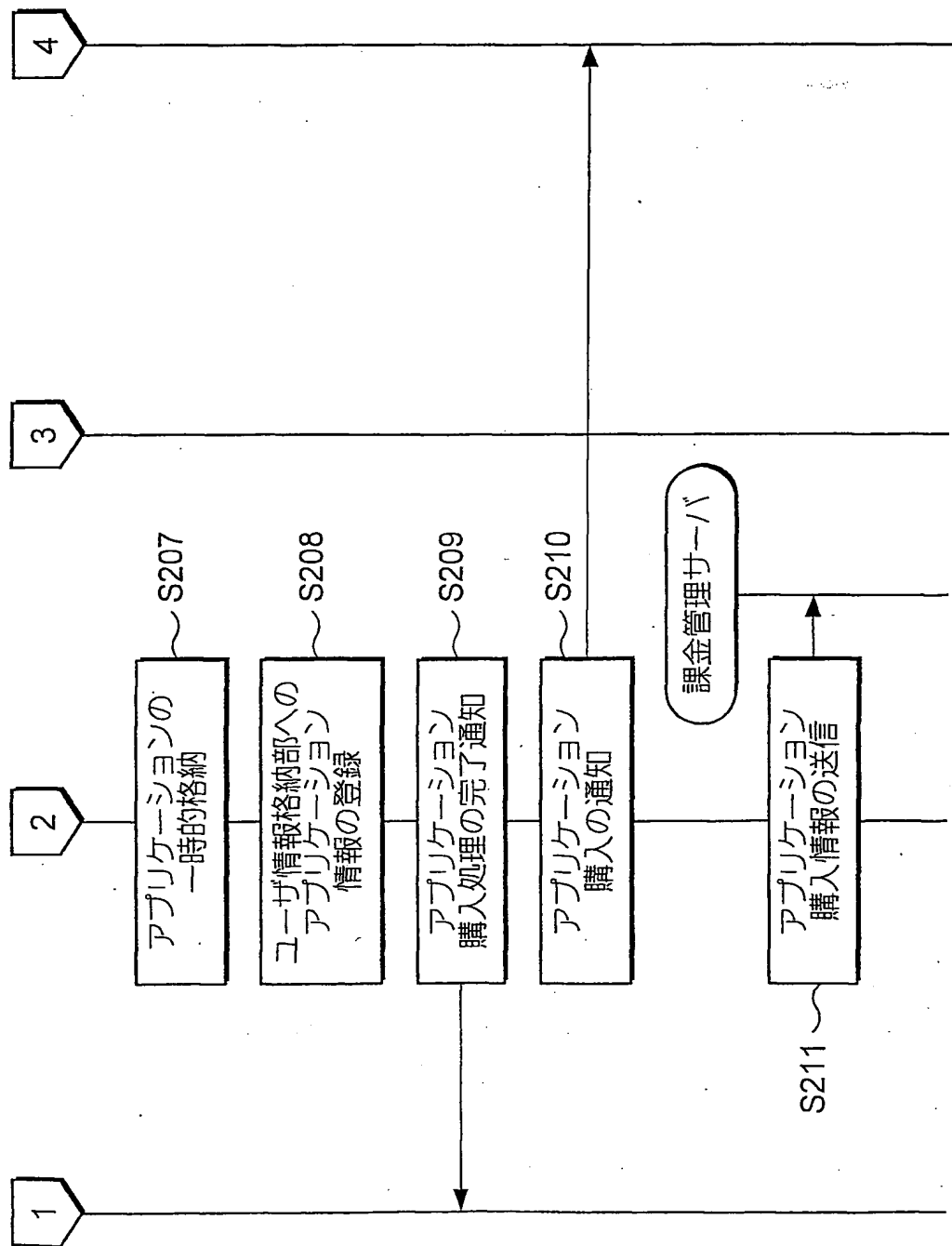


図 16

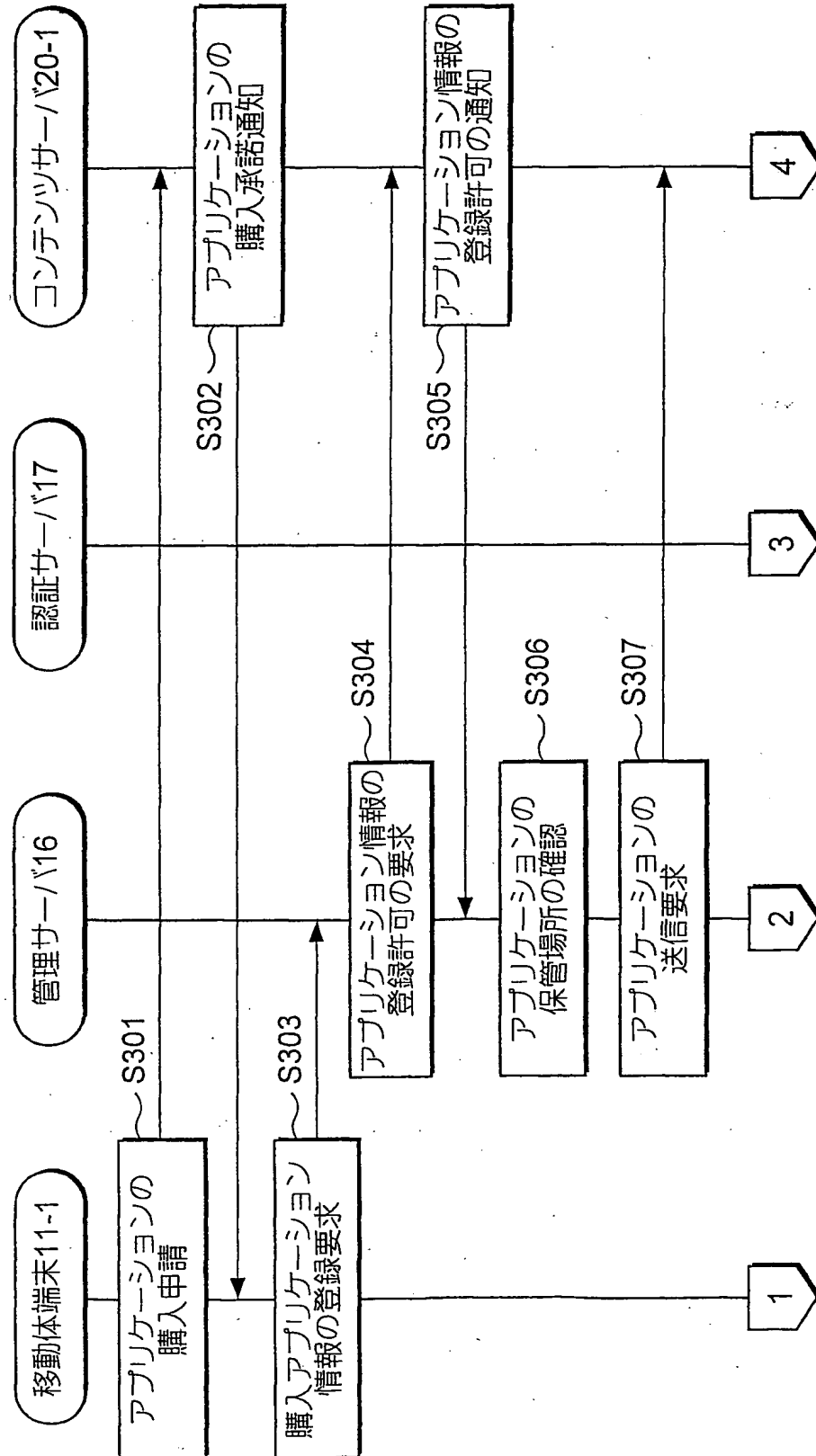
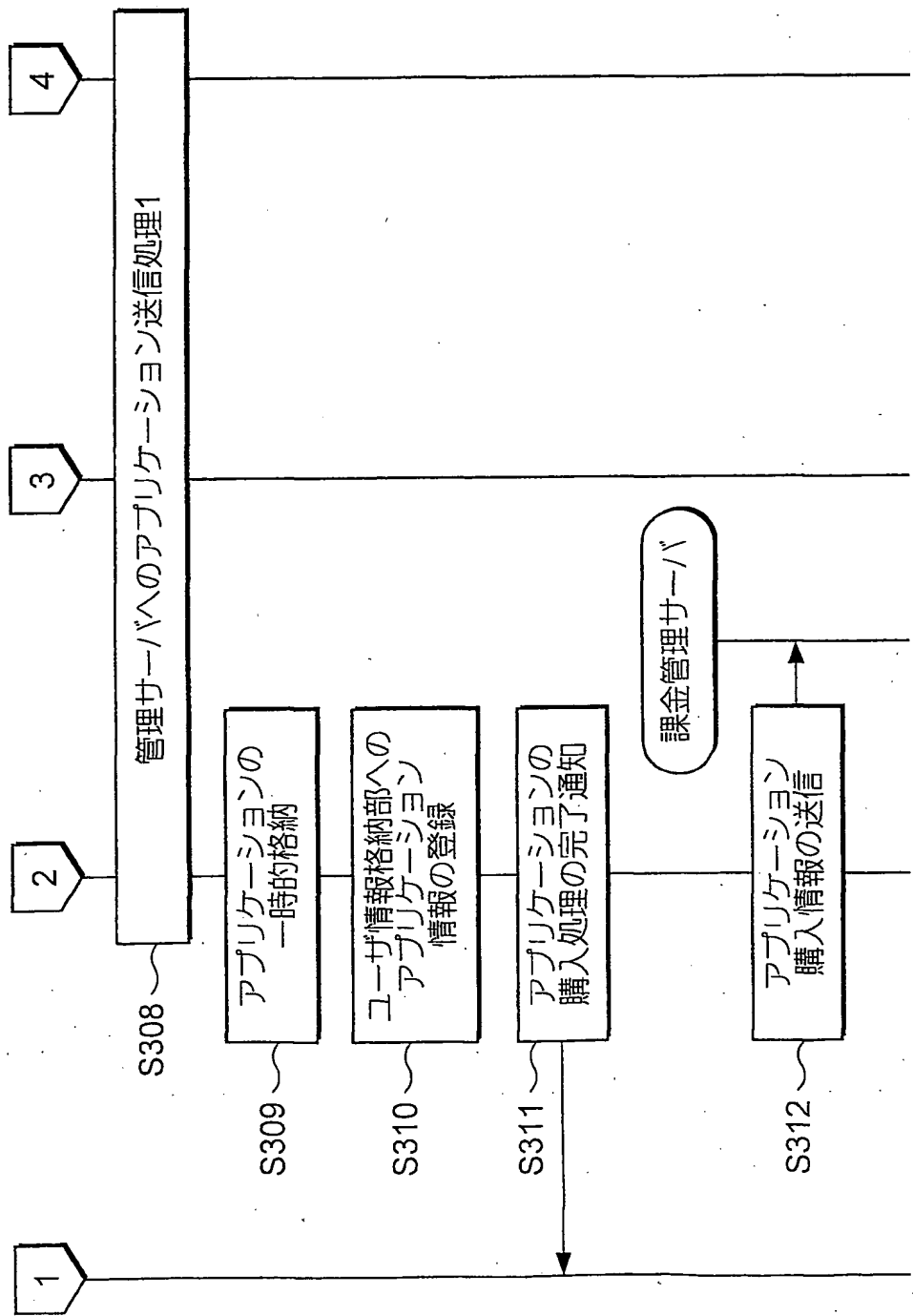


図 17



17/41

図 18

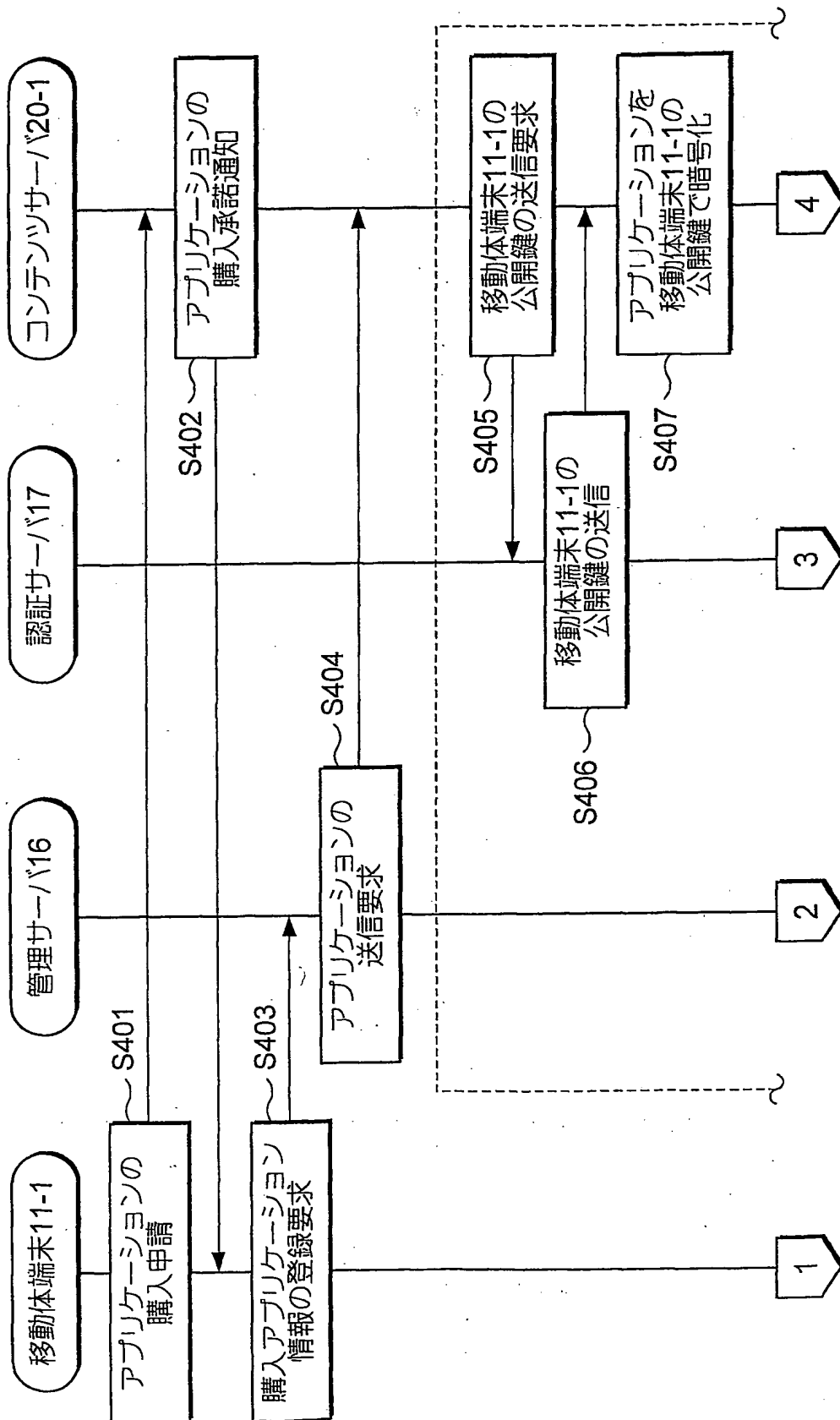


図 19

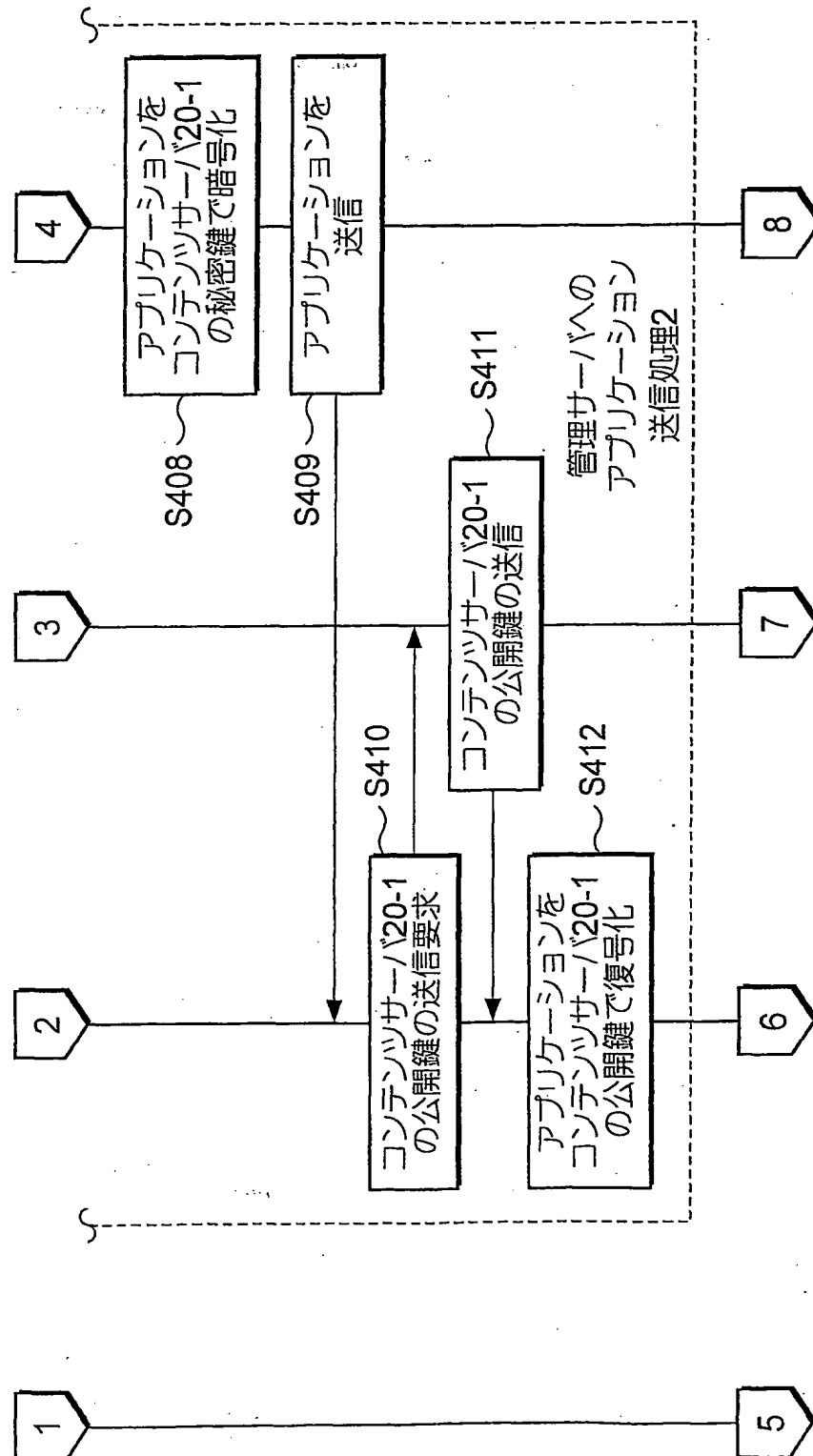


図 20

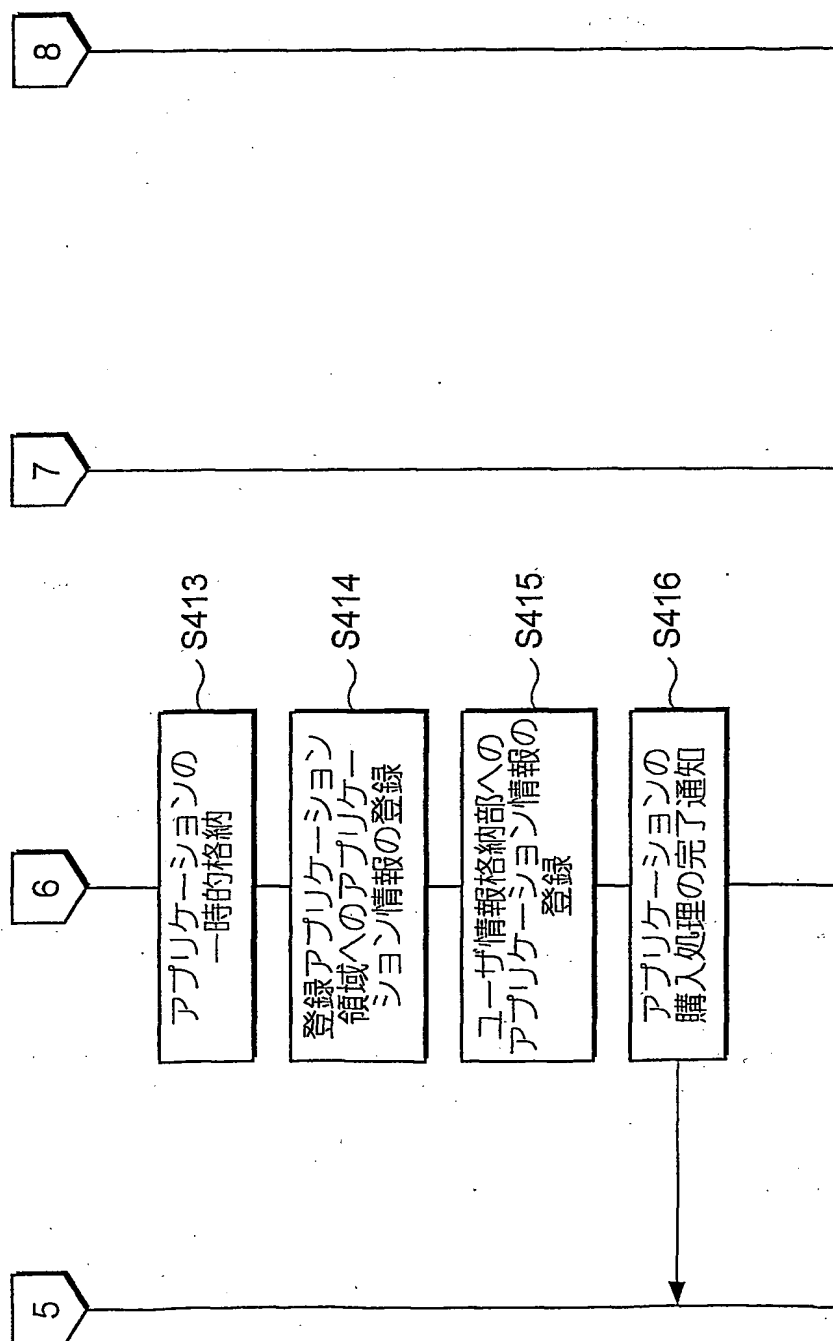


図 21

D21

## アプリケーションメニュー

1. アプリケーションの新規購入
2. アプリケーションのダウンロード
3. アプリケーションの起動
4. アプリケーションの解約
0. 前ページ

D23

メモリが不足しています。  
スケジュール管理 Ver. 2  
をダウンロードするために、現在メモリ  
にあるアプリケーションを削除する必  
要があります。

9. 実行
0. 前ページ

D22

## ダウンロード可能アプリケーション

1. スケジュール管理 Ver. 2
2. カードゲーム Ver. 3
3. 図形描画ツール Ver. 5
4. カード決済 Ver. 3
9. 次ページ
0. 前ページ

D24

削除するアプリケーションを選択してく  
ださい。

1. シューティングゲーム Ver. 7
2. eショッピング Ver. 5
3. 単語暗記ツール Ver. 3
4. 世界の時刻表示 Ver. 1
9. 次ページ
0. 前ページ



図 22

D25

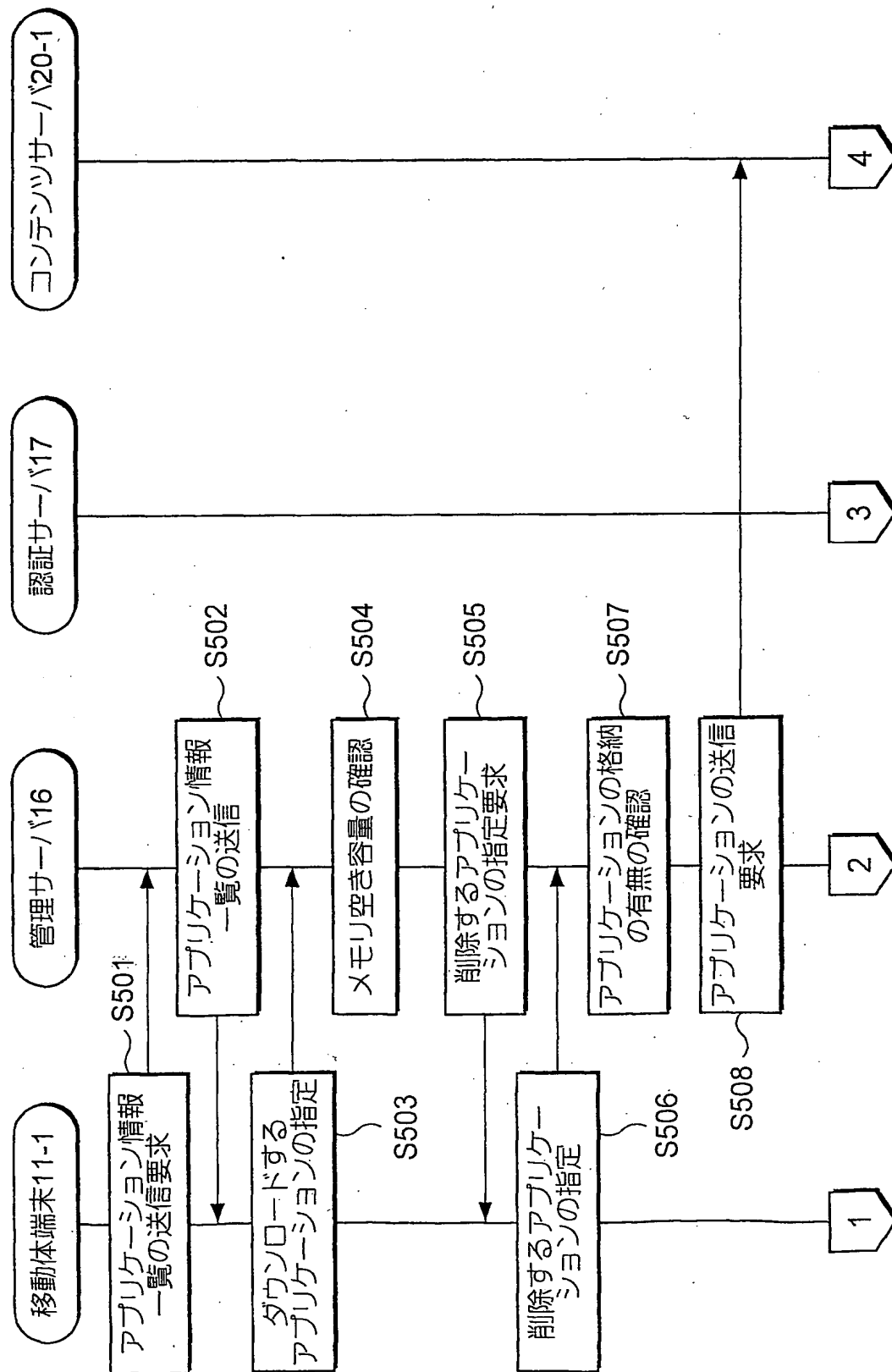
スケジュール管理 Ver. 2  
をダウンロード中です。  
しばらくお待ち下さい。

D26

電話番号

22/41

図 23





24/41

図 25

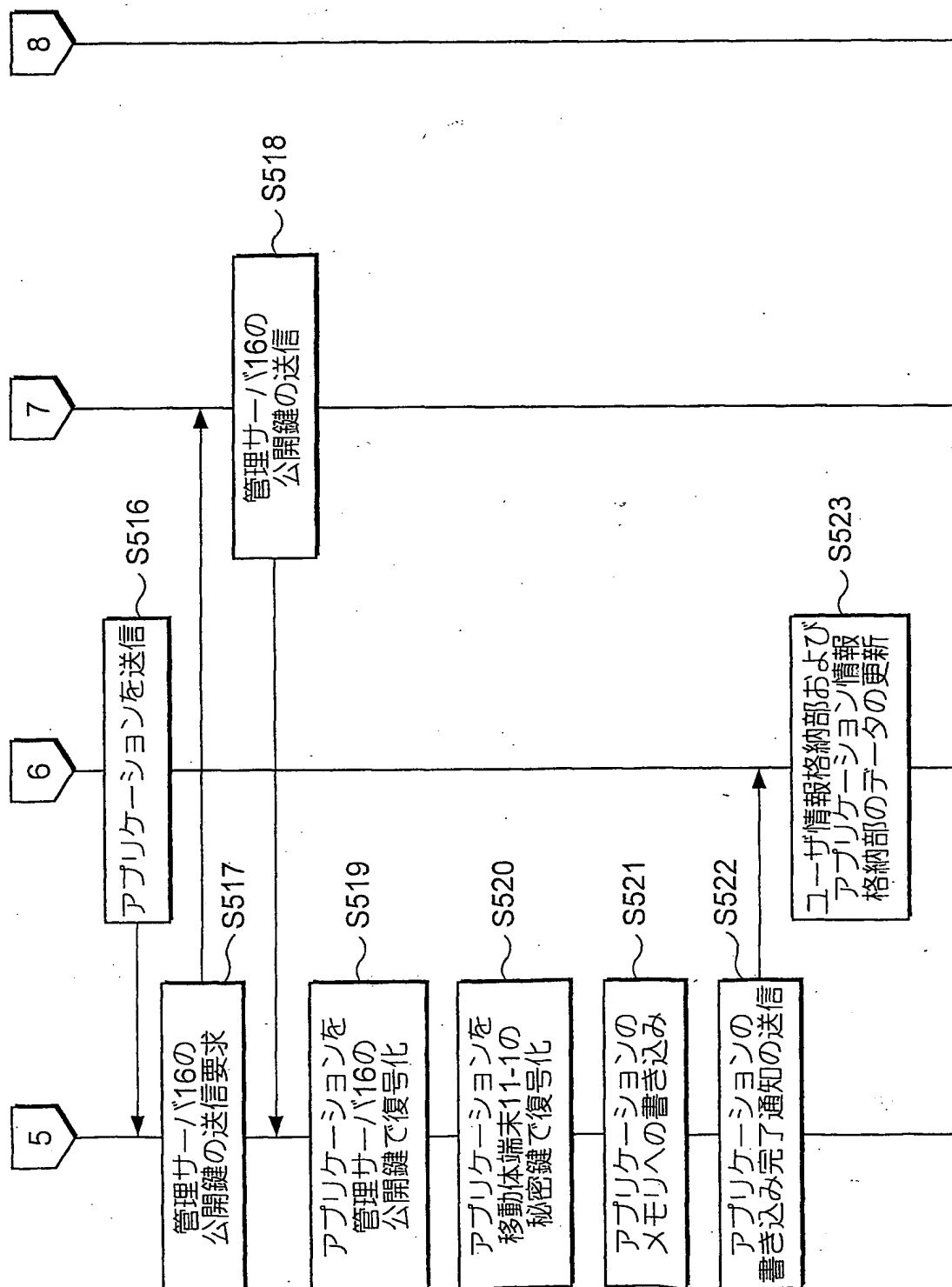
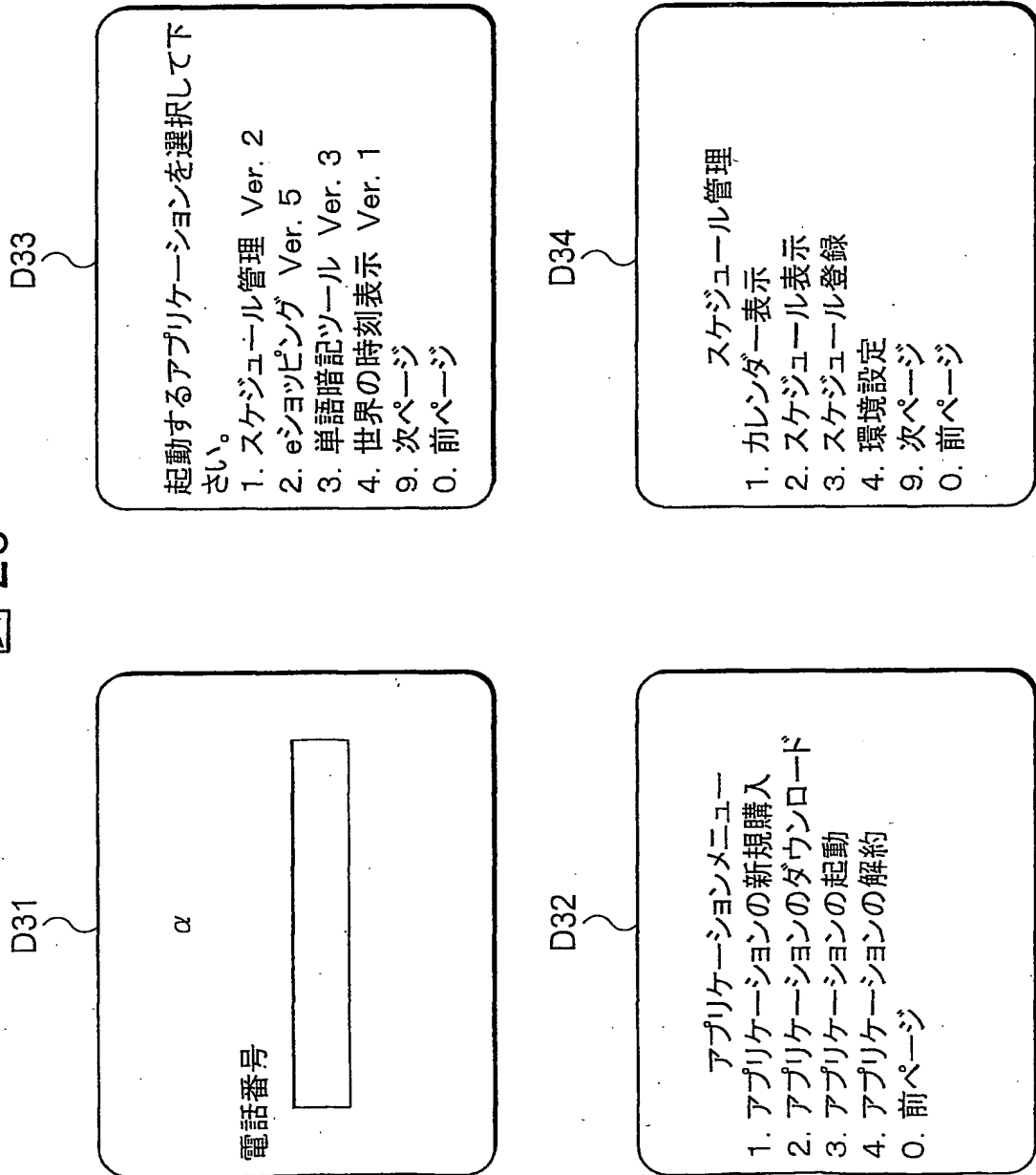


図 26



26/41

図 27

D41

## アプリケーションメニュー

1. アプリケーションの新規購入
2. アプリケーションのダウンロード
3. アプリケーションの起動
4. アプリケーションの解約
0. 前ページ

D43

## abc鉄道

1. 時刻表
2. 乗車券予約
3. 定期乗車券購入
4. 購入履歴閲覧
9. 次ページ
0. 前ページ

D42

起動するアプリケーションを選択して下さい。

1. 定期券アプリケーション abc鉄道
2. 決済アプリケーション xx銀行
3. 図形描画ツール Ver. 5
4. 世界の時刻表示 Ver. 3
9. 次ページ
0. 前ページ

D44

## abc鉄道 定期乗車券購入

- 利用区間  
[      ] 駅 - [      ] 駅
- 利用期間  
[    年 月 日 ] - [    年 月 日 ]
- 金額: [      ] 円
9. 次ページ
  0. 前ページ

図 28

D45

abc鉄道

定期乗車券の購入申込み処理が終了しました。

2001年5月15日までに料金を以下の口座に送金して下さい。

東京銀行 普通口座 54231687

9. 終了

0. 前ページ

D47

アプリケーションメニュー

1. アプリケーションの新規購入

2. アプリケーションのダウンロード

3. アプリケーションの起動

4. アプリケーションの解約

0. 前ページ

D46

電話番号

D48

起動するアプリケーションを選択して下さい。

1. 定期券アプリケーション abc鉄道

2. 決済アプリケーション xx銀行

3. 図形描画ツール Ver. 5

4. 世界の時刻表示 Ver. 3

9. 次ページ

0. 前ページ

図 29

D49

xx銀行  
普通口座 54987625  
暗証番号 [     ]  
9. 実行  
0. 前ページ

D51

xx銀行  
送金情報を入力して下さい。  
送信元:xx銀行 普通口座 54987625  
送信先:[     ]  
[     ]銀行 口座種別:[普通・当座]  
口座番号:[     ]  
送金額: 5,000円  
9. 実行 0. 前ページ

D50

xx銀行  
1. 口座開設  
2. 残高照会  
3. 送金  
4. 定期預金申込  
9. 次ページ  
0. 前ページ

D52

xx銀行  
入金処理を完了しました。  
照会番号: 257-624-567  
ご利用ありがとうございました。  
9. 終了  
0. 前ページ



図 30

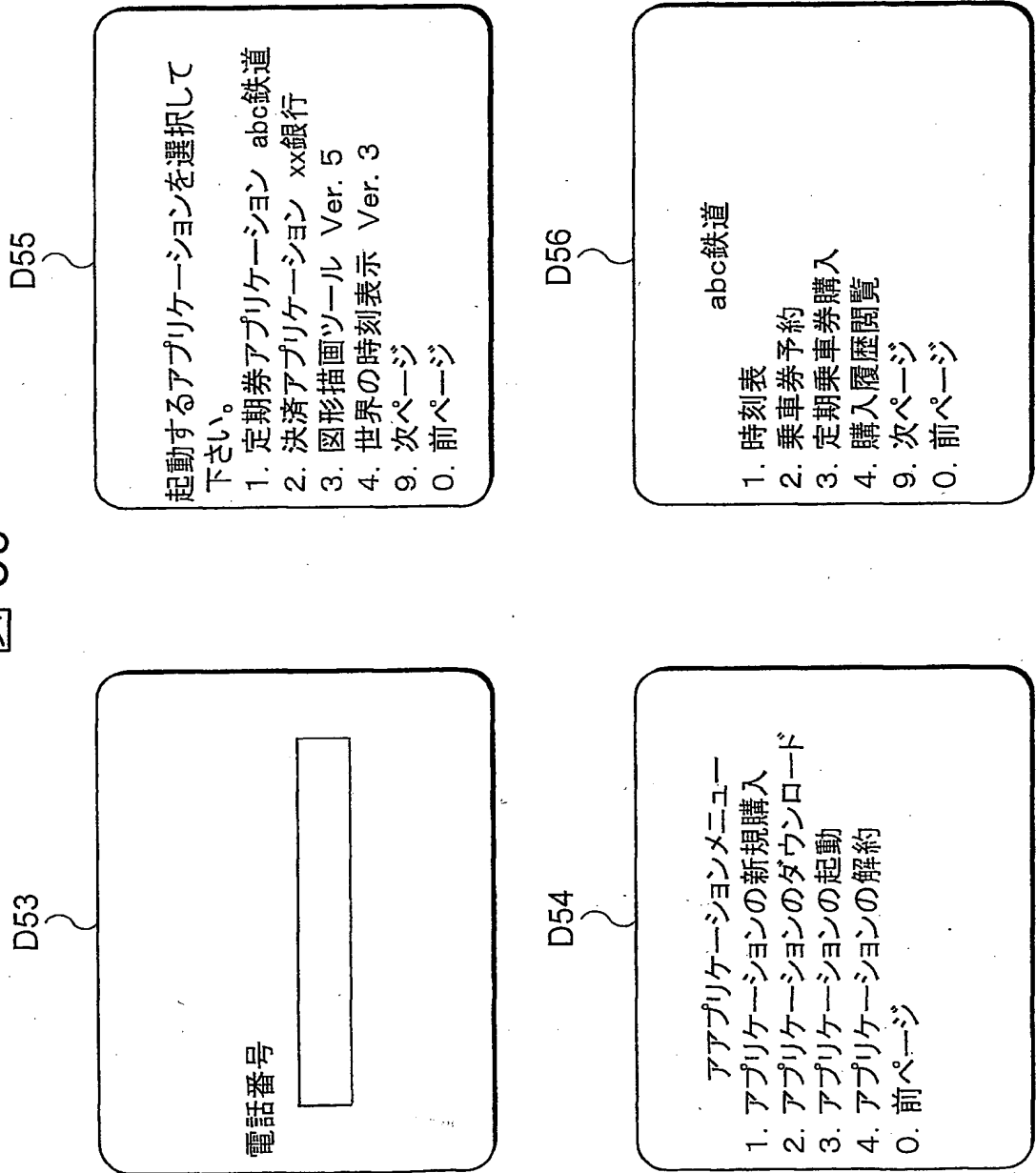


図 31

D57

abc鉄道

購入履歴一覧

- 1. 2001年5月8日 定期乗車券購入
- 2. 2001年3月10日 特急券予約
- 3. 2001年2月20日 乗車券購入

- 9. 次ページ
- 0. 前ページ

D58

abc鉄道

購入履歴詳細

- 2001年5月8日 定期乗車券購入
- 東京駅-新宿駅
- 2001年 5月16日-6月15日
- 送金確認済み

- 9. 終了
- 0. 前ページ

D59

電話番号

図 32

D71

アプリケーションメニュー

1. アプリケーションの新規購入
2. アプリケーションのダウンロード
3. アプリケーションの起動
4. アプリケーションの解約
0. 前ページ

D73

サイバー商店zz

購入する商品を選択して下さい。

1. 野菜セット5kg (2,000円)
2. 牛肉1kg (5,000円)
3. 特選地酒1本 (7,000円)
4. 果物セット5kg (4,000円)
9. 次ページ
0. 前ページ

D72

起動するアプリケーションを選択して下さい。

1. 通信販売アプリケーション サイバー商店zz

2. 決済アプリケーション xx銀行
3. クレジットアプリケーション cc信販
4. 決済アプリケーション kk銀行
9. 次ページ
0. 前ページ

D74

サイバー商店zz

商品の配送先を入力して下さい。

9. 次ページ
0. 前ページ

32/41

図 33

D75

サイバー商店zz  
決済方法を指定して下さい。

1. 決済アプリケーション xx銀行
3. クレジットアプリケーション cc信販
2. その他の決済方法

0. 前ページ

D77

xx銀行

送金情報を確認して下さい。  
送信元:xx銀行 普通口座 54987625  
送信先:サイバー商店zz  
nn銀行 普通口座 41256378  
送金額: 5,000円  
9. 確認  
0. 前ページ

D76

xx銀行  
普通口座 54987625  
暗証番号 [     ]

9. 実行  
0. 前ページ

D78

サイバー商店zz

送金を確認しました。  
商品のお届けは、2001年5月1日に  
なります。  
注文番号: 987-654-191  
ご利用ありがとうございました。  
9. 終了  
0. 前ページ

33/41

図 34

D79

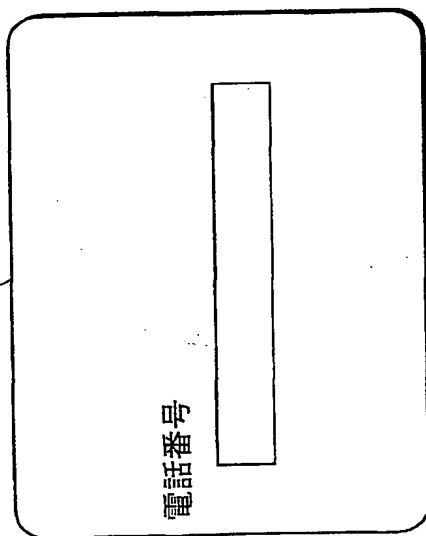


図 35

AP-3568からの要求				AP-3568への要求			
アプリケーション 読み取り	データ 読み取り	データ 書き込み	データ 削除	アプリケーション 読み取り	データ 読み取り	データ 書き込み	データ 削除
AP-3712	AP-8125	AP-1346	AP-2349	AP-4315	AP-1523	AP-2349	AP-3125
AP-0123	AP-5724	AP-2349	AP-1272	AP-2349	AP-0312	AP-8125	AP-6789
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

35/41

図 36

アプリケーション 識別番号	信頼関係情報				公開	料金 徴収	保管場所
	アプリケーション 読み取り	データ 読み取り	データ 書き込み	データ 削除			
AP-2568	AP-4315	AP-1523	AP-2349	AP-3125	Yes	Yes	アプリケーション本体を格納
	AP-2349	AP-0312	AP-8125	AP-6789			
	⋮	⋮	⋮	⋮			
AP-3712	AP-2436	AP-1297	AP-2635	AP-3251	Yes	No	ftp://ftp.abc_software.com/ application/ap_0306.exe
	AP-9870	AP-0879	AP-8187	AP-6789			
	⋮	⋮	⋮	⋮			
AP-4513	AP-9870	AP-9009	AP-7614	AP-1231	No	Yes	アプリケーション本体を格納
	AP-1121	AP-0012	AP-8198	AP-6763			
	⋮	⋮	⋮	⋮			
AP-3021	AP-4121	AP-1231	AP-1213	AP-9809	No	No	ftp://ftp.software_world.com/ software/app_view.exe
	AP-5454	AP-8192	AP-8125	AP-1265			
	⋮	⋮	⋮	⋮			
F-3251	—	—	—	—	—	—	ftp://ftp.softpocket.com/root/ app/miracle.exe
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

36/41

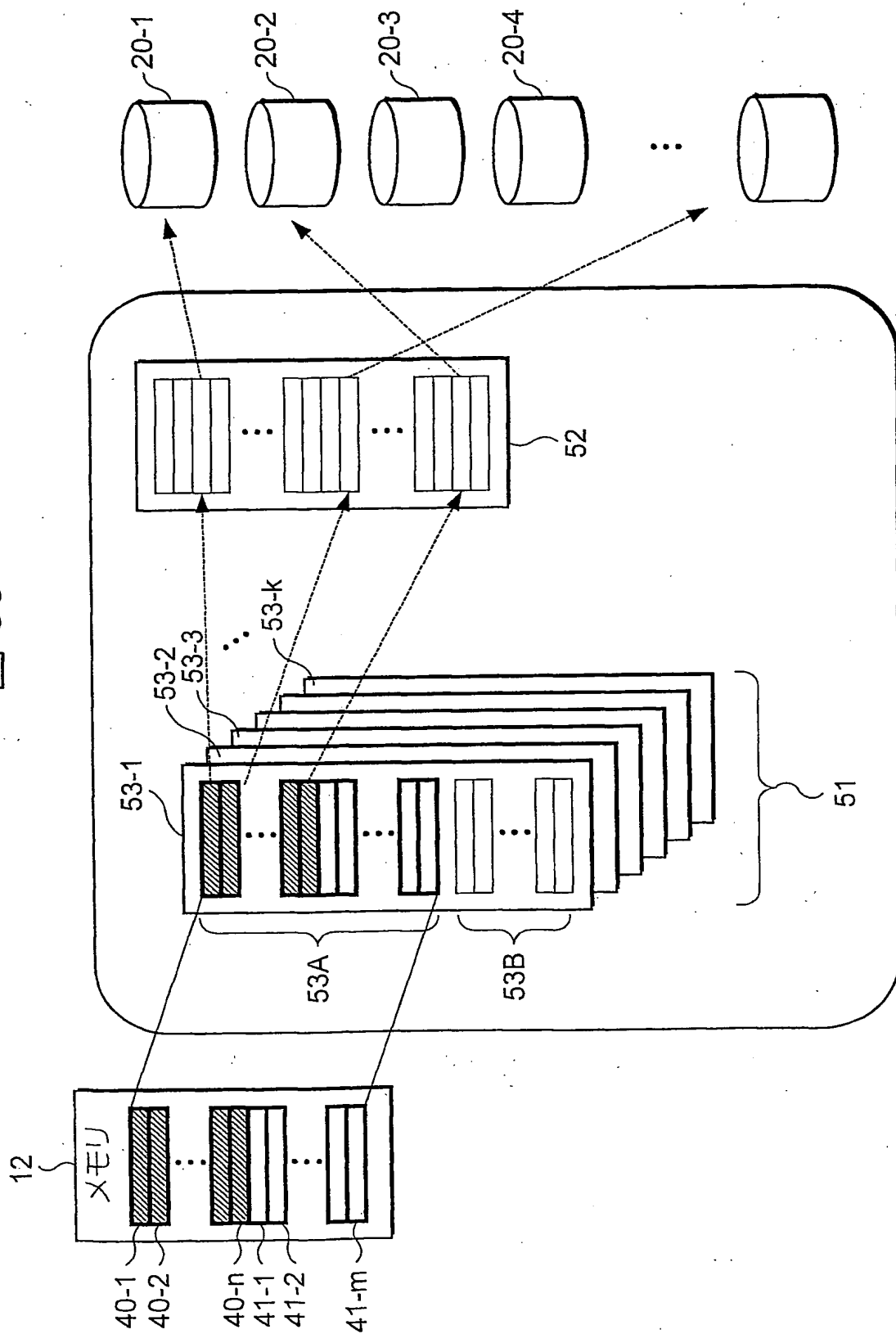
図 37

アプリケーション 識別番号	信頼度	料金徴収	保管場所	
AP-2568	3	Yes	ftp://ftp.neonetwork.com/public/apbinder.exe	内容証明書
AP-3712	5	No	ftp://ftp.abc_software.com/application/ap_0306.exe	内容証明書
AP-4513	2	Yes	ftp://ftp.humantec.com/mobile/application007.jar	内容証明書
AP-3021	1	No	ftp://ftp.software_world.com/software/app_view.exe	内容証明書
F-3251	0	—	ftp://ftp.softpocket.com/root/app/miracle.exe	内容証明書
⋮	⋮	⋮	⋮	⋮



37/41

図 38



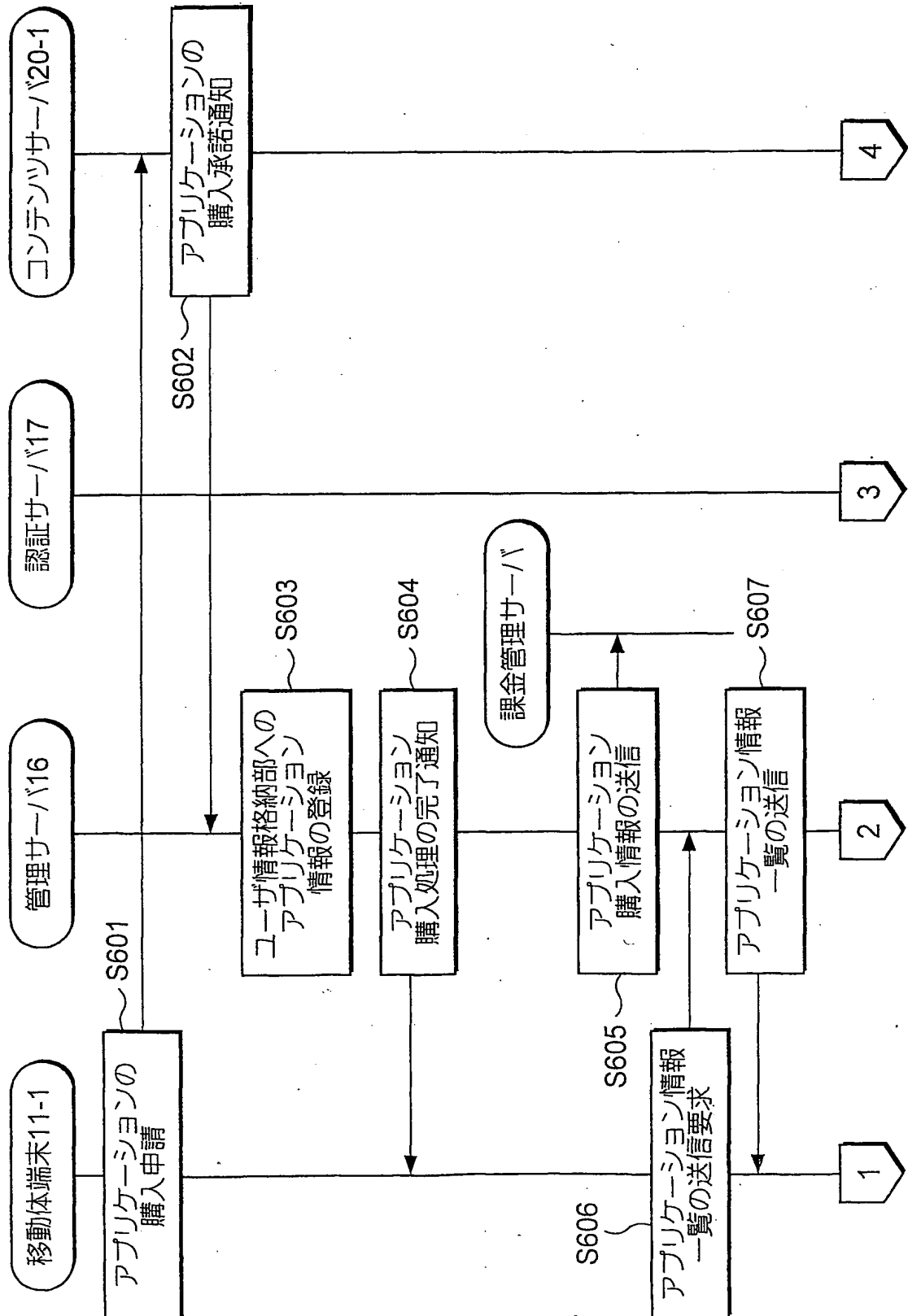
38/41

図 39

	メモリ エリア		アプリケーション 識別番号	アクティベーション
既配信アプリケーション領域	管理エリア	1	AP-2568	Yes
		2	AP-0123	No
		3	AP-1015	Yes
		⋮	⋮	⋮
		n	未使用	—
	フリーエリア	1	F-0325	Yes
		2	F-7485	Yes
		3	未使用	—
		⋮	⋮	⋮
		m	未使用	—
配信可能アプリケーション領域		1	AP-4125	—
		2	F-5963	—
		3	AP-3021	—
		4	AP-4513	—
		5	未使用	—
		6	未使用	—
		7	未使用	—
		8	未使用	—
		9	未使用	—
		⋮	⋮	⋮

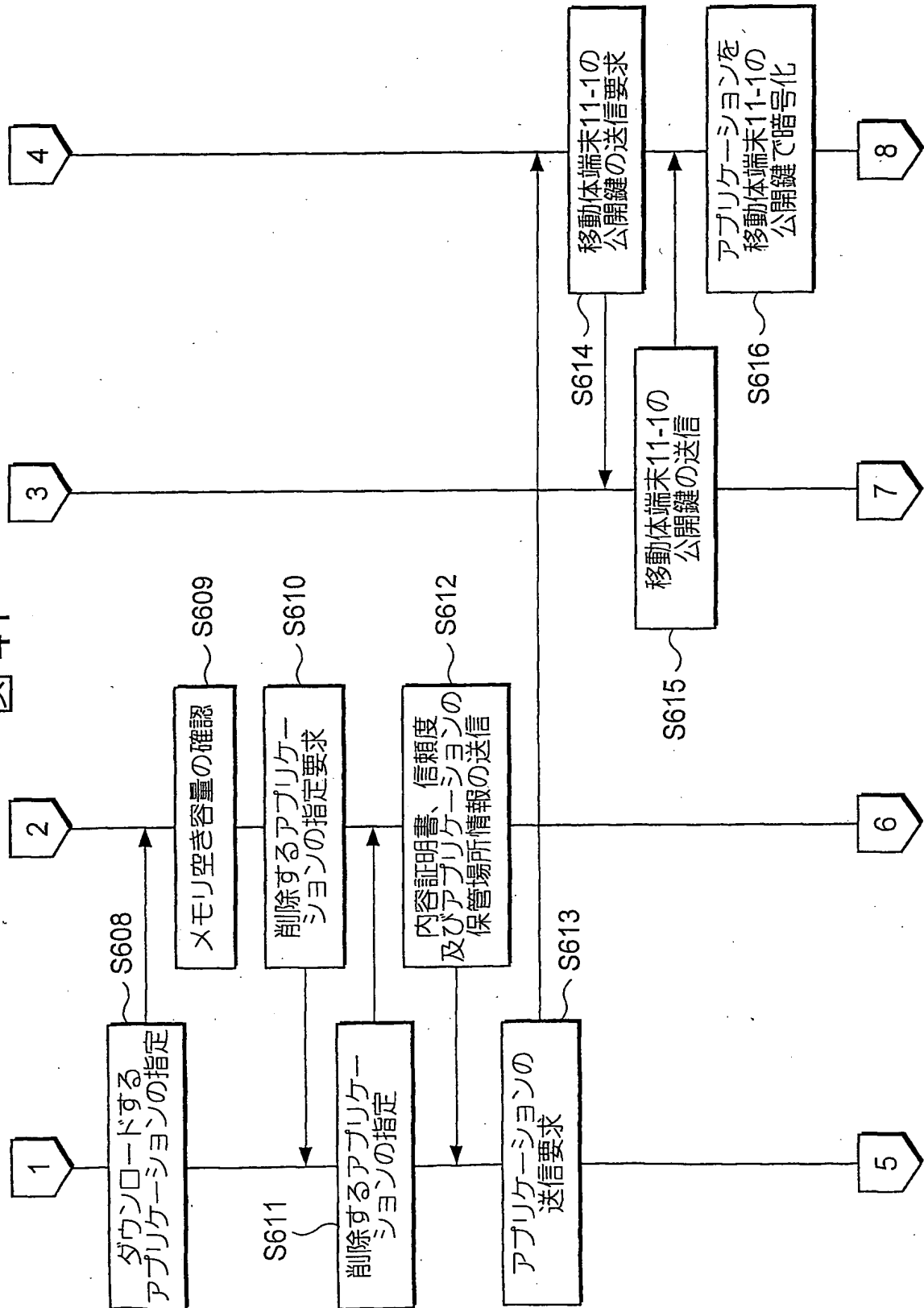
39/41

図 40



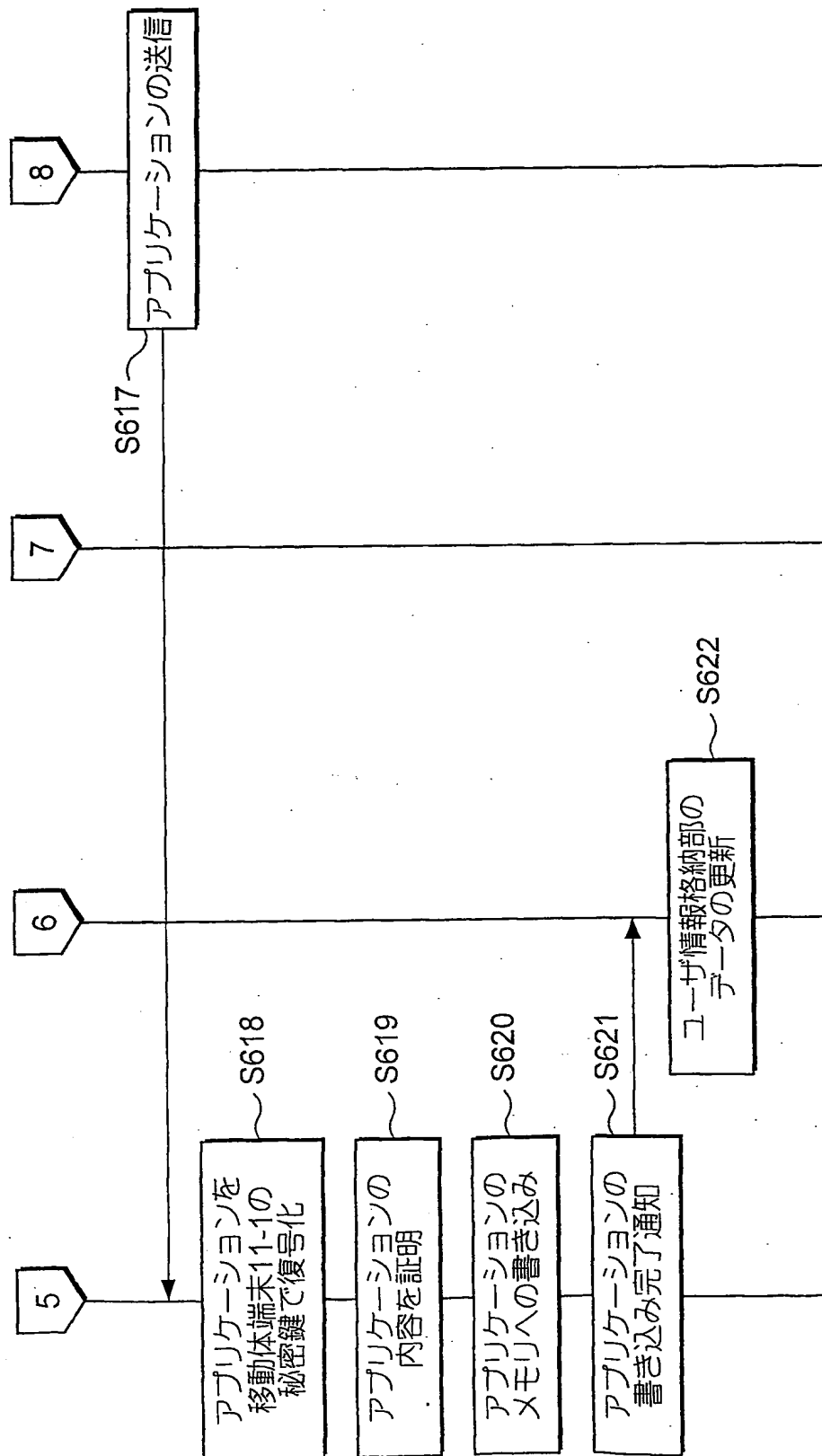
40/41

図 41



41/41

図 42



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/04643

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G06F9/06, G06F13/00, G06F9/445, G06F17/60, H04L9/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F9/06, G06F13/00, G06F9/445, G06F17/60, H04L9/10,  
G06F15/00, G06F15/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00/42498 A1 (Hitachi, Ltd.), 20 July, 2000 (20.07.00), Page 4, line 11 to page 5, line 26 & AU 1889699 A	1-3, 17, 18, 29, 30, 39, 41, 43, 45
X	EP 778522 A2 (Sun Microsystems, Inc.), 11 June, 1997 (11.06.97), Claims 1 to 14 & JP 10-69382 A	1-3, 17, 18, 29, 30, 39, 41, 43, 45
X	EP 813132 A2 (International Business Machines Corp.), 17 December, 1997 (17.12.97), Claims 1 to 17 & JP 10-83310 A & US 5825877 A	1-3, 17, 18, 29, 30, 39, 41, 43, 45

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:  
 "A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier document but published on or after the international filing date  
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search  
01 August, 2002 (01.08.02)

Date of mailing of the international search report  
13 August, 2002 (13.08.02)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/04643

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 813133 A2 (International Business Machines Corp.), 17 December, 1997 (17.12.97), Claims 1 to 16 & JP 10-91427 A	1-3, 17, 18, 29, 30, 39, 41, 43, 45
Y	WO 00/42498 A1 (Hitachi, Ltd.), 20 July, 2000 (20.07.00), Page 4, line 11 to page 5, line 26 & AU 1889699 A	4-12, 19-24, 31-36, 40, 42, 44, 46
Y	EP 778522 A2 (Sun Microsystems, Inc.), 11 June, 1997 (11.06.97), Claims 1 to 14 & JP 10-69382 A	4-12, 19-24, 31-36, 40, 42, 44, 46
Y	EP 813132 A2 (International Business Machines Corp.), 17 December, 1997 (17.12.97), Claims 1 to 17 & JP 10-83310 A & US 5825877 A	4-12, 19-24, 31-36, 40, 42, 44, 46
Y	EP 813133 A2 (International Business Machines Corp.), 17 December, 1997 (17.12.97), Claims 1 to 16 & JP 10-91427 A	4-12, 19-24, 31-36, 40, 42, 44, 46
Y	JP 2-122330 A (Hitachi, Ltd.), 10 May, 1990 (10.05.90), Page 3, lower left column, last line to lower right column, line 5; page 4, upper right column, lines 4 to 7, 18 to lower left column, line 3 (Family: none)	8, 9, 23
Y	JP 9-244900 A (Taito Corp.), 19 September, 1997 (19.09.97), Page 5, right column, lines 42 to 45; page 6, left column, lines 36 to 38; right column, lines 19 to 23, 32 to 42; page 7, left column, lines 2 to 4; page 10, left column, lines 37 to 39; page 12, right column, lines 2 to 10 (Family: none)	8-12, 23, 24, 35, 36
A	JP 8-249312 A (Xing Inc. et al.), 27 September, 1996 (27.09.96), Page 8, left column, lines 21 to 24 (Family: none)	13-16, 25-28, 37, 38
Y	EP 875815 A2 (Sony Corp.), 04 November, 1998 (04.11.98), Refer to figures 3(102), 14, 16(94) and the explanations thereof. & JP 10-301772 A	4-7, 19-22, 31-34, 40, 42, 44, 46

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP02/04643

C (Continuation): DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-117885 A (NTT Comware Corp.), 27 April, 2001 (27.04.01), Page 5, left column, lines 1 to 24 (Family: none)	4-7, 19-22, 31-34, 40, 42, 44, 46



## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F9/06, G06F13/00, G06F9/445, G06F17/60,  
H04L9/10

## B. 調査を行った分野

## 調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F9/06, G06F13/00, G06F9/445, G06F17/60,  
H04L9/10, G06F15/00, G06F15/16

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
日本国公開実用新案公報 1971-2002年  
日本国登録実用新案公報 1994-2002年  
日本国実用新案登録公報 1996-2002年

## 国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WO 00/42498 A1 (株式会社日立製作所) 2000.07.20, 第4頁第11行~第5頁第26行。 & AU 1889699 A	1-3, 17, 18, 29, 30, 39, 41, 43, 45
X	EP 778522 A2 (SUN MICROSYSTEMS, INC.) 1997.06.11, 請求項1~14。 & JP 10-69382 A	1-3, 17, 18, 29, 30, 39, 41, 43, 45

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

## の日の後に公表された文献

- 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

01.08.02

国際調査報告の発送日

13.08.02

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

久保 光宏



5B

9189

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	EP 813132 A2 (International Business Machines Corporation) 1997. 12. 17, 請求項1~17。 & JP 10-83310 A & US 5825877 A	1-3, 17, 18, 29, 30, 39, 41, 43, 45
X	EP 813133 A2 (International Business Machines Corporation) 1997. 12. 17, 請求項1~16。 & JP 10-91427 A	1-3, 17, 18, 29, 30, 39, 41, 43, 45
Y	WO 00/42498 A1 (株式会社日立製作所) 2000. 07. 20, 第4頁第11行~第5頁第26行。 & AU 1889699 A	4-12, 19-24, 31-36, 40, 42, 44, 46
Y	EP 778522 A2 (SUN MICROSYSTEMS, INC.) 1997. 06. 11, 請求項1~14。 & JP 10-69382 A	4-12, 19-24, 31-36, 40, 42, 44, 46
Y	EP 813132 A2 (International Business Machines Corporation) 1997. 12. 17, 請求項1~17。 & JP 10-83310 A & US 5825877 A	4-12, 19-24, 31-36, 40, 42, 44, 46
Y	EP 813133 A2 (International Business Machines Corporation) 1997. 12. 17, 請求項1~16。 & JP 10-91427 A	4-12, 19-24, 31-36, 40, 42, 44, 46
Y	JP 2-122330 A (株式会社日立製作所) 1990. 05. 10, 第3頁左下欄末行~第3頁右下欄第5行、第4頁右上欄第4~7 行、第4頁右上欄第18行~第4頁左下欄第3行 (ファミリーな し)	8, 9, 23
Y	JP 9-244900 A (株式会社タイトー) 1997. 09. 19, 第5頁右コラム第42~45行、第6頁左コラム第36~38行、 第6頁右コラム第19~23行、第6頁右コラム第32~42行、 第7頁左コラム第2~4行、第10頁左コラム第37~39行、第 12頁右コラム第2~10行 (ファミリーなし)	8-12, 23, 24, 35, 36
A	JP 8-249312 A (株式会社エクシング、外1名) 1996. 09. 27, 第8頁左コラム第21~24行 (ファミリーなし) (特別ページに続く)	13-16, 25-28, 37, 38

引用文献のカテゴリー：Y

引用文献名：EP 875815 A2 (SONY CORPORATION)

1998.11.04,

第3図の102、第14図、第16図の94と、それらの説明文参照。

& JP 10-301772 A

関連する請求の範囲の番号：4-7, 19-22, 31-34, 40, 42, 44, 46

引用文献のカテゴリー：Y

引用文献名：JP 2001-117885 A

(エヌ・ティ・ティ・コムウェア株式会社)

2001.04.27,

第5頁左コラム第1~24行 (ファミリーなし)

関連する請求の範囲の番号：4-7, 19-22, 31-34, 40, 42, 44, 46